FIRST-STRIKE ADVANTAGE: THE UNITED STATES' COUNTER TO CHINA'S PREEMPTIVE INTEGRATED NETWORK ELECTRONIC WARFARE STRATEGY

BY

MAJOR CHANTEL M. BOOKER

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE
First-Strike Advantage: The United States' Counter To China's Preemptive Integrated Network Electronic Warfare Strategy

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Air and Space Studies,,Air University,,Maxwell Air Force Base,,AL

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study aims to assess the advantage of the United States??? adopting a first-strike stratagem in cyberspace for confronting China???s first-strike stratagem. The most likely scenario for this stratagem is if China decides to invade Taiwan, they will likely strike at US logistics and command and control infrastructure preemptively in order to delay and inhibit a US response. Analyzing both China and the Unites States??? political and military aims as well as the states??? cyber capabilities provides a foundation for analyzing the specific context of a stratagem. In order to determine the usefulness of a first-strike stratagem in cyberspace, the study first analyzes the conditions for a first-strike advantage with nuclear weapons as well as space weapons. These conditions and the characteristics of the weapons themselves are then compared to the conditions of war in cyberspace and cyber weapons to determine how a first-strike stratagem would be advantageous in cyberspace. This study has several findings. First, the first-strike advantage of cyber weapons compared to nuclear weapons is vastly different and results in a first-strike stratagem using cyber weapons for deterrence as not useful. Second, a first-strike advantage is gained when countering cyber weapons and some conventional weapons. Third, first-strike in cyberspace is likely to be the most useful for coercion by denial, less useful for coercion via risk, and least useful for coercion through punishment. Fourth, a first-strike stratagem fits very well with US strategic and military aims, although a declaratory stratagem aimed at deterrence is not useful in cyberspace, one that is not declared could be very useful. Fifth, technology and cyberspace is continuously changing, which will affect the future usefulness of a first-strike stratagem for deterrence. As a result of these findings, it is recommended the United States adopt a non-declaratory first-use stratagem aimed at countering the use of China???s cyber weapons or conventional weapons with an option to use cyber weapons in a first-strike for coercion by denial. The adoption of a first-use stratagem for countering the use of China???s cyber weapons or conventional weapons fits the nature of the weapon as well as current US political and military aims.

15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT **unclassified**	b ABSTRACT **unclassified**	c THIS PAGE **unclassified**	**Same as Report (SAR)**	**112**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

EVERETT C. DOLMAN (Date)

_____

SUZANNE C. BUONO (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Chantel M. Booker received a Bachelor of Science Degree in Electrical Engineering, as well as her commission as a Second Lieutenant, in 1999 from the University of Nebraska-Lincoln. She also received a Master's Degree in Business Administration from the University of Nebraska-Lincoln in 2002. As a cyber operations officer, Major Booker has completed assignments in the United States, Pacific, and Middle East. In 2011, Major Booker attended Air Command and Staff College in Maxwell AFB, AL, graduating in the top 15 percent of her class, and then attended the School for Advanced Air and Space Studies (SAASS) the following year. Upon graduation from SAASS, Major Booker will be assigned to Beale AFB as the 9th Communications Squadron Commander.

ACKNOWLEDGMENTS

I owe tremendous thanks to Dr. Everett Dolman, my thesis advisor, for the guidance, support, thought provoking conversations, and critical analysis of my work. I would also like to thank Colonel Suzanne Buono for her valuable insights and ensuring the final product was as good as I could make it. Dr. Jeffrey Reilly and Dr. James Tucci helped with the topic selection and getting me started in the right direction. I also owe a debt of gratitude to Class XXII and the faculty. Each of them has added to my year at SAASS, broadened my perspective and challenged my ways of thinking. I am a better person for having spent this year with them.

Finally, I owe an immeasurable debt of gratitude to my family. Thank you and I love you to my husband, mother, father, and my brother, whom all provided much needed encouragement over the course of the year—especially when I secluded myself with research and a computer during much of the family holiday gathering. To my husband, I am truly blessed to have you by my side and appreciate everything you did to make this year easier—I am sure I owe you at least a few rounds of golf!

ABSTRACT

This study aims to assess the advantage of the United States' adopting a first-strike stratagem in cyberspace for confronting China's first-strike stratagem. The most likely scenario for this stratagem is if China decides to invade Taiwan, they will likely strike at US logistics and command and control infrastructure preemptively in order to delay and inhibit a US response. Analyzing both China and the Unites States' political and military aims as well as the states' cyber capabilities provides a foundation for analyzing the specific context of a stratagem. In order to determine the usefulness of a first-strike stratagem in cyberspace, the study first analyzes the conditions for a first-strike advantage with nuclear weapons as well as space weapons. These conditions and the characteristics of the weapons themselves are then compared to the conditions of war in cyberspace and cyber weapons to determine how a first-strike stratagem would be advantageous in cyberspace. This study has several findings. First, the first-strike advantage of cyber weapons compared to nuclear weapons is vastly different and results in a first-strike stratagem using cyber weapons for deterrence as not useful. Second, a first-strike advantage is gained when countering cyber weapons and some conventional weapons. Third, first-strike in cyberspace is likely to be the most useful for coercion by denial, less useful for coercion via risk, and least useful for coercion through punishment. Fourth, a first-strike stratagem fits very well with US strategic and military aims, although a declaratory stratagem aimed at deterrence is not useful in cyberspace, one that is not declared could be very useful. Fifth, technology and cyberspace is continuously changing, which will affect the future usefulness of a first-strike stratagem for deterrence. As a result of these findings, it is recommended the United States adopt a non-declaratory first-use stratagem aimed at countering the use of China's cyber weapons or conventional weapons with an option to use cyber weapons in a first-strike for coercion by denial. The adoption of a first-use stratagem for countering the use of China's cyber weapons or conventional weapons fits the nature of the weapon as well as current US political and military aims.

CONTENTS

Chapter		Page
	DISCLAIMER	ii
	ABOUT THE AUTHOR	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	INTRODUCTION	1
1	DEFINITIONS AND CONCEPTS REGARDING CYBERSPACE	6
2	CHINA	32
3	UNITED STATES	48
4	FIRST-STRIKE STRATAGEMS	60
5	FIRST STRIKE COMPARISONS	77
6	RECOMMENDATIONS	97
	BIBLIOGRAPHY	99

Illustrations

Figure		
1	US DOD War-fighting Domains	14
2	JP 3-13 Definitions	17
3	Factors to Consider for a Cyber Attack Meeting Use of Force Threshold	27
4	General Staff Department of the People's Liberation Army	39
5	Timeline of Significant Chinese-Related Cyber Events from 1999-2009	45
6	Seven Policy Priorities for the International Strategy for Cyberspace	54

Introduction

Background and Strategic Implications

China's capabilities in cyberspace have grown significantly over the last ten years, as have attacks on United States networks attributed to China.[1] The increase in network attacks is primarily due to a combination of China's improved capabilities and the People's Liberation Army's (PLA) aggressive strategy in cyberspace. Formally, the Chinese government states its overall military strategy is one of active defense and state they will not use offensive means unless attacked first. However, the former director of the PLA's Communications Department, Major General Dai Qingmin, advocates something quite different than a strategy of active defense. General Dai Qingmin has written several articles advocating preemptive cyber-attacks to gain the initiative and seize information superiority.[2] Although preparing for offensive action in case of attack is in line with active defense, infiltrating adversarial networks and preplacing cyber weapons is preemptive and not in line with a strategy of active defense. Furthermore, in addition to advocating a preemptive strategy for cyberspace, China's actions in cyberspace indicate this is indeed its current strategy.

The continued dispute over Taiwan and its independence is a potential flashpoint in relations between the United States and China. If China decided to invade Taiwan, it is highly probable its leaders would preemptively launch a cyber attack on the United States to prevent or limit intervention. In fact, US officials fear the most sophisticated threat the country faces would come from China.[3] Benjamin Lambeth points out how severe the consequences of hostile action in cyberspace may be, stating, "Opponents who would exploit opportunities in cyberspace with hostile intent have every possibility for adversely affecting the very livelihood of the Nation, since that area has increasingly become not just the global connective tissue, but also the Nation's central nervous system

[1] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," (DTIC Document, 2009), 67.
[2] D. Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare," *Journal of Defence Studies* 4(2010): 30.
[3] Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Force Quarterly* 60(2011): 51.

and center of gravity."[4] General Cartwright further points out American reliance on cyberspace stating, "90% of American business connects and does essential communications in cyberspace."[5] Furthermore, the PLA has noted US reliance upon cyberspace and the potential vulnerabilities associated with this reliance. It has specifically noted any defense of Taiwan by the United States will rely upon the speed of its response and ability to provide adequate forces. The PLA has identified US logistics and command and control infrastructures as US strategic centers of gravity. It is very likely it will likely seek to degrade those systems early in a conflict.[6] Adding to the problem of US dependency is the probability that preemptive attacks may not be readily detected until after the attacks have been fully executed. Then, if definitive attribution is lacking, no policy exists to determine the appropriate response.

While most of the strategic guidance published by US leaders is defensive in nature, President Obama has recently declared a preemptive policy in regards to cyberspace.[7] The United States DOD Defense Strategy for Operating in Cyberspace states, "the DOD will treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential . . . In the case of a contingency involving network failure or significant compromise, DOD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations."[8] The recent declaration of preemption in cyberspace adds offensive options for US decision makers and strategists to an otherwise defensive strategy.

Thesis and Methodology

China's distinct change from active defense to a first-strike strategy regarding cyber is something the United States should seriously consider in regards to its own

---

[4] Lambeth, "Airpower, Spacepower, and Cyberpower," 50.
[5] General James E. Cartwright, "Comments" (paper presented at the Air Force Association Air Warfare Symposium, 8 February 2007).
[6] B. Krekel, P. Adams, and G. Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," (US-China Economic and Security Review Commission. Northrup-Grumman, 2012), 9.
[7] David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*(2013), http://www nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=1&_r=1&ref=us (accessed 17 February 2013).
[8] W. Lynn and J. Cartwright, "Defense Strategy for Operating in Cyberspace," (2011).

strategy. This is an important consideration given the United States' recent shift to a first-strike stratagem.[9] I will consider how a first-strike stratagem is useful in countering China's first-strike stratagem and make a recommendation regarding the best use of a stratagem in the current context. I have broken this thesis into six chapters to evaluate the relevant factors of a first-strike stratagem in cyberspace.

Chapter 1 sets the foundation of the paper by examining and explaining strategy as well as the relatively new war-fighting domain of cyberspace. This sets a common framework for understanding what strategy is and is not as well as what cyberspace is and is not. In this chapter, I explain the unique attributes of cyberspace, which both aid and hinder operations in cyberspace and effect what a cyber war looks like. These attributes are key to understanding what makes a first-strike stratagem useful in cyberspace.

Chapter 2 provides foundational information about China. It examines China's view of the world, its strategic goals, and its overall military goals. It then expands upon these goals to explain China's thoughts about cyberspace, its capabilities, and its cyber strategy. This provides the basis for understanding how cyber fits into China's broader military strategy.

Chapter 3 provides information about the United States. Similar to the chapter on China, it examines the United States' strategic and military goals as well as its cyberspace strategy and capabilities. From an understanding of US strategic and military goals, I can later evaluate the utility of a first-strike stratagem in accomplishing them. Furthermore, by understanding the declared US cyber strategy and understanding the United States' cyber capabilities, I can better determine how first-strike fits and what is and is not possible with respect to a first-strike stratagem.

Chapter 4 analyzes the concept of a first-strike advantage using two previously studied case studies and determines the surrounding conditions that make the stratagem effective. It also explains the foundational knowledge of deterrence and compellence strategies to aid in this understanding. The first case is a first-strike stratagem using nuclear weapons. I examine the conditions for a first-strike advantage by using the Cold War as a historical example, nuclear deterrence theory, and the properties of a nuclear

[9] Sanger and Shanker, "Broad Powers Seen for Obama in Cyberstrikes".

weapon. The second case is the weaponization of space and examines under what conditions a first-strike stratagem would be advantageous. I examine deterrence theory as well as the properties of a potential space weapon for determining the conditions surrounding a first-strike advantage in space. The advantageous conditions for each case can then be compared to the conditions in cyberspace to derive when a first-use stratagem would be useful.

Chapter 5 is divided into two sections to first compare the advantageous conditions of nuclear first-strike and second, compare the advantageous conditions of a space first-strike to the conditions of and attributes of cyberspace. Additionally, I also consider the context of both the United States' and China's strategy and capabilities when drawing these parallels. Then, I consider how this stratagem meets the overall goals and tone of US political and military strategy. Finally, I consider how future improvements to attributing actions in cyberspace could affect the usefulness of the stratagem.

Chapter 6 provides a first-strike stratagem recommendation based upon the analysis in Chapter 5.

Assumptions:

Cyber is a legitimate war-fighting domain. In addition to being able to create physical effects as the Stuxnet virus did, cyberspace weapons can create non-kinetic effects as well.[10] The additions of data or affecting the integrity of data are two examples often overlooked by military professionals traditionally focused on kinetic effects.

This analysis will only cover state-sponsored actions. Non-state-sponsored hackers, or individuals, will not be considered in the analysis of a first-strike stratagem. Although cyberspace has given individuals and small groups increasing influence, it is not relevant in regards to analyzing the stratagems of China and the United States.

I have assumed the arguments for assured destruction and the first-strike policy in nuclear deterrence are valid. I based this upon the historical evidence of the Cold War between the Soviet Union and the United States, which did not invalidate this theory.

Unresolved legal problems in cyberspace have been limited to problems that will slow the decision making response process. The specific legal problems, such as what to

[10] Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare (New York: Penguin Press, 2011), 103.

do and who is responsible if State A attacks State B through State C, are not part of this analysis.

Limitations:

There are limitations to the types of documents available regarding Chinese strategy. The Chinese government limits the type of information publicly available concerning its military strategy. Facts about specific capabilities and infrastructure are difficult to find. Thus, I derived many of their capabilities from various PLA exercises. China's 2010 National Defense White Paper and various articles written by Chinese PLA Generals, translated on www.opensource.gov, are the primary sources of information concerning their strategy.

The second limitation is that these and other documents have been translated from the Chinese language. Strategists could further misconstrue any mistakes in translation or things that simply do not translate well into poor strategy decisions. Furthermore, these primary source documents have been the foundation of much of the recent writing on this topic, which results in very similar findings and conclusions. To add to the problem, most of the publications are made by a small group of scholars.

The third limitation is the limited amount of information regarding United States Cyber strategy due to the infancy of cyberspace. JP3-12 Cyberspace Operations does not exist as of 15 April 2013.

The fourth limitation is the number of intermingled policies regarding cyber that must be resolved. Examples include legal policies regarding attack through sovereign countries, what the United States or the international community considers an attack in cyberspace, as well as what is a proportional response in cyberspace. These are all potential topics for future research.

The fifth limitation of this analysis is that there are currently no known weapons in space; thus, the arguments for a first-strike advantage are purely theoretical but based upon what is scientifically possible.

Chapter 1

Definitions and Concepts Regarding Cyberspace Strategy

Cyberspace is a relatively new war-fighting domain with a wide variety of contrasting views of what it is and how to operate in it. Thus, defining a common framework of terms for this new domain is necessary in order to determine whether, and if so *how* a first-strike stratagem in cyber will be useful in countering China's first-strike stratagem. First, I show that understanding military strategy and its differentiation from tactics is the base of the framework for developing a stratagem. Then I assert that differentiating cyberspace from the other war-fighting domains is fundamental to the proper utilization of the domain in warfare. While cyberspace and the air, land, sea, and space domains share some similarities, it is also very different from them. Understanding the unique attributes of cyberspace helps make the proper parallels of how the military fights in the other domains to cyberspace, while avoiding incorrect parallels. Building upon this framework, the distinction between operations in cyberspace, communications, and the electromagnetic spectrum (EMS) becomes clear. This distinction helps narrow down what a first-strike stratagem includes and assists in understanding how China's views of cyberspace differ from those of the United States. Finally, I explain what cyber power, cyber attack, and cyber war are in order to illustrate the benefits as well as the difficulties of operating in this domain.

Military Strategy

In order to develop a stratagem for cyberspace, I begin by defining the broader concept of military strategy. Military strategy is often a misunderstood concept. It is commonly defined as how to use the available means to reach an assigned goal or end state. However, this use of the ends-ways-means construct actually describes tactics, which contributes to the corruption of strategy's definition.[1] Thus, a helpful way of understanding strategy and deriving a definition of it is by differentiating it from tactics.

[1] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 15.

The first differentiation of strategy from tactics is best made by the influential Prussian theorist, Carl Von Clausewitz, who defined strategy as "the use of engagements for the object of war" and tactics as "the use of armed forces in the engagement."[2] Based upon these definitions, strategy encompasses tactics: "The original means of strategy is victory–that is, tactical success; its ends, in the final analysis, are those objects which directly lead to peace."[3] At the tactical level, armed forces are the means used in an engagement. Their purpose is to win the engagement.[4] At the strategic level, the engagements are the means to achieve the purpose of the war. The strategic purpose of war, according to Clausewitz, is "to attain a better state of peace."[5] At the strategic level, this better state of peace does not necessarily require the armed forces to win every engagement. It may not require the armed forces to win any of them.[6]

Second, strategy is continuous and evolving and does not have a distinct end state because the strategist is trying to achieve an enduring or ongoing advantage, while tactics always has an end state because the tactician is striving for a result.[7] Strategy, unlike tactics, does not end simply because a war or battle has concluded. Similar to how politics continue after a war ends, so does strategy. Another way to view this is that strategy must continue because not every war leads to a permanent settlement, and even when it does, unless one side is completely destroyed or incorporated into the political structure of the winning state, relations between them will go on.[8] Tactics, on the other hand, does have a distinct end and ceases when the engagement or warfare ceases. Thus, military strategy must always be forward looking and adaptive as the environment changes to fulfill the continuous political aim of the state through times of peace and war. Furthermore, since strategy is continuous, strategists must describe it qualitatively rather than quantitatively. Strategists must become comfortable with notions of better or worse; they must be patient and have faith in the ultimate direction of their planning, the

---

[2] Carl von Clausewitz, *On War* (Princeton, N.J.: Princeton University Press, 1984), 128.
[3] Clausewitz, *On War*, 143.
[4] Clausewitz, *On War*, 143.
[5] Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, 15. Dolman was paraphrasing from Clausewitz, *On War*, 143.
[6] This was the case in the Vietnam War. The US won every battle, but the Vietnamese won the war. See Phillip Davidson, *Vietnam at War: 1946-75* (New York: Oxford University Press, 1991), ix.
[7] Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, 11.
[8] Clausewitz, *On War*, 90.

eventual better state of peace. A quantitative description gives over too easily for measurable markers of success that tug at strategy and make it indistinguishable from tactics—it allows strategy to end once military forces reach the prescribed quantity.[9] Tacticians, on the other hand can, quantify ends in order to maximize efficiency in reaching them. In order to move on to another mission or objective, they need a quantified or measurable end state for the current one. They need a defined outcome toward which to strive.

Finally, strategy is about *manipulating the structure and context of conflict* within which military commanders make decisions, and formulate and execute tactics. If tactics is about matching means, ways, and ends, strategy is about acquiring and providing the necessary means, establishing the enforcing the proper ways, and determining the essential ends. A strategist will change and adapt rules, policies, rules of engagement (ROEs), and regulations to alter the structure of a conflict. For example, the ROEs may state military forces must gradually escalate any use of force in conflict. In this case, a plane may fly over an engagement as a show of force, then escalate by dropping flares, and then further escalate by dropping bombs. If the ROEs change, then the environment for the tacticians as well as the opponent also changes. If a graduated escalation of force is no longer required, the strategy used by the opponent may shift if it knows it may not have the warning provided by something like a fly over. By changing the contextual factors, "the strategist may provide additional options to the opponent, inducing the other side to make a decision that was not previously apparent, but now seems necessary."[10]

From these characteristics, the definition of strategy I will use is "managing context for continuing advantage in the pursuit of policy."[11] To summarize, strategy is continuous, qualitative in nature, and used to achieve political aims, which provides the state a continuing advantage. Additionally, strategy should always present more options by manipulating the context and structure of the conflict.

---

[9] Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, 12. Again, Vietnam is a useful metaphor. The US used tactical results to justify strategy. It must have been winning because the tactical measure of success—body counts—was overwhelmingly in its favor. Indeed, the major turning point of the war, the Tet Offensive, was a tactical victory for the US, but it was an essential part of the North's strategy to wear down America's resolve. J. Proctor, *American Resolve and the Art of War: A Study and Application of Military Tactics* (Bloomington, IN: Author House, 2012), 10.
[10] Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, 43.
[11] Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, 19.

Cyberspace

Cyberspace has become increasingly important as more hardware and systems become networked together and made reliant upon cyberspace. Since its inception, the definition of cyberspace has evolved over time with different people and organizations each highlighting a different aspect of what they believe cyberspace is. First, I will show a variety of cyberspace definitions from different sources across time, highlighting their evolution and the differences between how they are perceived. Second, I will briefly explain the two predominant models most definitions of cyberspace follow and then show how the US DOD's definition follows the inclusive model. Third, I compare the US DOD's definition of cyberspace to definitions of other domains in order to consider how a more useful and consistent definition of cyberspace should be constructed. The resulting definition parallels how the US DOD defines the other domains, differing only to highlight its *unique* aspects. From this definition, I show how cyberspace fits as a domain for military operations, fully nested within the proper role of strategy described above but carefully differentiated for its unique characteristics, which allows for tailoring a distinct cyberspace strategy. Finally, I describe the purpose of cyberspace strategy, which in turn provides the logic for developing a first-strike stratagem.

The variety of definitions, in addition to the many changes in definitions over time, highlights the difficulty of conceptualizing what cyberspace is. The definitions range from calling cyberspace a consensual hallucination to the online world of computer networks with some variations in-between. Among them are:

- William Gibson, who coined the term cyberspace in his cyberpunk novel, *Neuromancer,* called it "a consensual hallucination."[12]

- Edward Waltz, says the "Cyberspace dimension refers to the middle layer—the information infrastructure—of the three realms of the information warfare battlespace. These three realms are the physical (facilities, nodes), the information infrastructure, and the perceptual.[13]

- "Cyberspace is that intangible place between computers where information momentarily exists on its route from one end of the global network to the other . . . the ethereal reality, an infinity of electrons

[12] William Gibson, *Neuromancer* (New York: Ace, 1984), 51.
[13] Edward Waltz, *Information Warfare: Principles and Operations* (Boston, MA: Artech House, 1998), 27, 150.

speeding down copper or glass fibers at the speed of light . . . Cyberspace is borderless . . . [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."[14]

- "The notional environment within which electronic communication occurs."[15]

- "Cyberspace . . . [it is the] environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web."[16]

- "Cyberspace is the information space consisting of the sum total of all computer networks."[17]

- "the on-line world of computer networks."[18]

The variety appears daunting, but John Sheldon simplifies the myriad through categorization and asserts there are two predominant models scholars and professionals use when defining cyberspace.[19] The inclusive model defines cyberspace by identifying (including) the hardware infrastructure that allows for the creation, maintenance, and promulgation of cyber activities, emphasizing the *physical* or real-world aspects of cyberspace. On the other hand, the exclusive model essentially ignores the infrastructure, focusing instead on the countless interactions of individuals within cyber networks and the information stored and manipulated there—the *virtual* place within the infrastructure. Perhaps because it is more comfortable with the tangibility of warfare, the US DOD's definition of cyberspace follows the inclusive model: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks,

---

[14] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1995), 49, 127.
[15] John A Simpson, E.S. Weiner, and Michael Proffitt, *Oxford English Dictionary* (Oxford, England: Clarendon Press, 1997).
[16] Walter Gary Sharp, *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research Corp., 1999), 15.
[17] Dorothy Elizabeth Robling Denning, *Information Warfare and Security* (New York: ACM Press, 1999), 22.
[18] Philip Babcock Gove, *Merriam Webster's Third New International Dictionary* (Springfield, MA: Merriam-Webster, 2002).
[19] J.B. Sheldon, "State of the Art: Attackers and Targets in Cyberspace," *Strategic Studies Quarterly* (2012): 3.

computer systems, and embedded processors and controllers."[20] This inclusive definition of cyberspace provides a comfortable target set for military tacticians, but misses the true essence of cyberspace and diverges from how US DOD defines the other war-fighting domains of land, sea, air, and outer space.

Of note, the DOD definition misses the essence of cyberspace by limiting it to the physical components used to create and manipulate cyberspace. The physical objects used to create the domain are not the domain themselves. They are enablers to action. They allow access to the domain much in the same way that aircraft and support bases allow access to the air domain, or rockets, satellites, launch facilities, and the like allow access to the space domain. Just as defining the sea domain by enumerating and classifying ships, submarines, naval aircraft, ports, and other instruments associated with ocean travel, or worse, describing the physical characteristics of seawater (its salinity, density, and other hydraulic properties) would miss the essence of what *seapower* is, so too is the essence of cyberpower lost through inclusive definitions of the domain.

Cyberspace describes the flow of data through a set of interconnected computers.[21] Cyberspace differs from the other domains in the regard that it is partially manmade and partially naturally existing, although at least conceptually, as described below, this is a matter of degree.[22] Cyberspace is partially manmade because the infrastructure, rules, and routing are manmade things necessary for data to flow. Cyberspace naturally exists in part because the data uses the electromagnetic spectrum (EMS) to flow. The space created by the infrastructure and the EMS, where the data flows, is cyberspace. Put in more eloquent terms, "Cyberspace is the proverbial ether within and through which electromagnetic radiation is propagated."[23]

Thus, the inclusive model used by the US DOD diverges from how it defines the other domains. Defining cyberspace as computers and processors is comparable to defining the air domain as an airplane, defining the space domain by spacecraft and

---

[20] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 16 November 2009. And Air Force Doctrine Document 3-12, *Cyberspace Operations*, 30 November 2011, 1. follow the joint definition.
[21] Terry Flew, *New Media: An Introduction* (New York: Oxford University Press, 2002).
[22] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 30.
[23] Lambeth, "Airpower, Spacepower, and Cyberpower," 50.

satellites, or defining the sea domain by ships and submarines. While it is obvious in these cases the air, space, and sea domains are not these physical items, for some reason the US DOD has defined cyberspace as such. The airplane, space shuttle, and satellites are what allow us to use and operate in the air and space domains. Similarly, the physical components simply allow us to use and operate in cyberspace, and to a greater extent than the others, to create the domain, but they are not the domain themselves.

A better definition of cyberspace will be similar to how JP 1-02 defines the other four war-fighting domains, yet distinguishes it from the other domains. The other domains are described in Figure 1. JP 1-02 does not specifically define the land domain.

Differentiation of Terms

Cyber and communications as well as cyberspace operations and electronic warfare (EW) are sets of terms that are often confused when studying and operating in the realm of cyber. The US DOD has interchangeably used the first set of terms, cyber and communications, contributing to the confusion between the two. The second set, cyberspace operations and EW, have similarities and synergies, which have led some scholars and professionals to argue they should be merged into one concept.[24] Examining the similarities and differences will show the distinction between the two. These similarities and differences will be integral to my analysis of China's integrated electronic network warfare approach in Chapter 3.

Cyber and communications are different concepts, but many people have misunderstood cyber as the new term for communications. Cyber includes "networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[25] As such, the term cyber generally covers computers and networks. In contrast, communication is the *exchange* of information. People can exchange information in cyberspace via computers, but they can also exchange information electronically via radios, satellites and telephones, or through non-electronic means such as courier, post, signaling, or simply talking face-to-face. Thus, cyber is a specific *type* of communications using computers and computer networks.[26]

The United States Air Force in particular blurred the distinction between cyber and communications when it changed the duty title of its communications officers to cyber operations officers in 2010. Although the duty title changed, indicating the officers' mission is specifically cyber operations, the mission did not change nor did the core of the officers' initial training. Instructors at the Undergraduate Cyber Training school still train Air Force officers to operate and maintain cyber, radio, phones, and

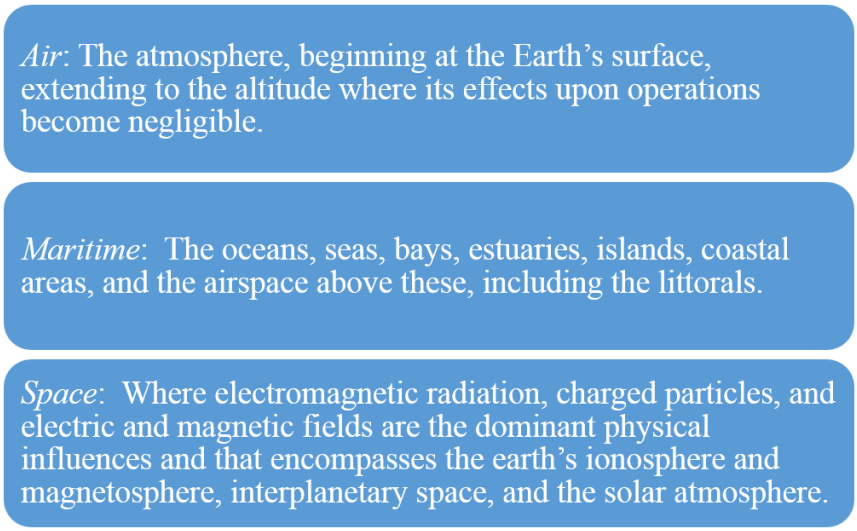
---

[24] Nurgul Yasar, Fatih M. Yasar, and Yucel Topcu, "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield" (paper presented at the Proc. of SPIE Vol, 2012); Jonathan W. Greenert, "Imminent Domain," *Proceedings Magazine* 138/12/I,318(2012), http://www.usni.org/magazines/proceedings/2012-12/imminent-domain (accessed 6 April 2013).
[25]JP Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 16 November 2009.
[26] Joint Publication 6-0, *Joint Communications System*, 10 June 2010, II-2.

satellite communications.[27] Although intended to highlight the importance of cyber operations within the communications field, the duty title change had another, more important intended effect. Air Force leaders changed the title so officers would begin to see their job as independently operational, and not strictly as mission support. "'It's not just spray paint, it's a new mindset,' said Brig. Gen. David Cotton, director of cyberspace transformation and strategy at the Air Staff."[28] This title change, although advantageous for changing a cultural mindset from support to operations, has many people believing cyber is the new name for communications, which is not helpful. If leaders use cyber in such a broad sense to cover *everything* involving communications and information technology, it adds to the confusion of what cyber is and is not; and worse, to what falls within the operational boundaries of the new cyber mindset.

Moreover, EW and cyberspace operations have both commonalities and differences in the US DOD. The primary difference between cyber operations and electronic warfare is their distinct missions defined in Figure 2.

Figure 1: US DOD War-fighting Domains



Source: Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 16 November 2009.

[27] Undergraduate Cyber Training Plans 2009 & 2010.
[28] "U.S. Air Force shifts 30,000 troops to 'cyberwar front lines'," *Homeland Security News Wire*(2010), http://www.homelandsecuritynewswire.com/us-air-force-shifts-30000-troops-cyberwar-front-lines (accessed 2 February 2013).

In each of these definitions, JP 1-02 defines the domain by what it is bounded by and what the military forces operate in and through. This does have its limitations, as there is considerable overlap in the domains, but it is less restrictive and more intuitively useful than a definition consisting of a list of things that operate in relation to it. A proposed definition of cyberspace that follows this pattern is "*the proverbial ether within and through which electromagnetic radiation is propagated to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*."[29] This definition of using electronics and the EMS to create, store, modify, exchange, and exploit information is a more precise, descriptive, and meaningful way of elaborating on the earlier description of cyberspace as the flow of data through an interconnected set of computers. It describes what the data flow is doing in the space created by the infrastructure and EMS, what the forces operate in and through, which *is* cyberspace.

This definition of cyberspace also shows how it is distinct from the other four war-fighting domains by its characterization, use of technology, and manipulation of information. First, cyberspace is distinct from the other domains because it is characterized by omnidirectional movement in the EMS and computer networking.[30] The laws of physics governing cyberspace are related to electromagnetism and light where cyberspace is the proverbial ether within and through which electromagnetic radiation is propagated.[31] Information in cyberspace is able to move nearly instantaneously via electromagnetic radiation across vast distances on a virtually unlimited number of fronts.[32]

---

[29] This definition is a combination of Lambeth's definition "Cyberspace is the proverbial ether within and through which electromagnetic radiation is propagated." Lambeth, "Airpower, Spacepower, and Cyberpower," 50; and Kuehl's definition, which puts more clarity into the first definition: "a global domain within the information environment whose distinct and unique character is framed by the use of electronics and the EMS to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

[30] Martin C. Libicki, "Military Cyberpower," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 276.

[31] Lambeth, "Airpower, Spacepower, and Cyberpower," 50.

[32] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 255; Lambeth, "Airpower, Spacepower, and Cyberpower," 53.

The concept of networking is important because it narrows down what is and what is not cyberspace. Cyber itself commonly means "of, relating to, or involving computers or computer networks"[33] and "virtual reality."[34] This concept of networking means there must be a means for multidirectional communication via interdependent and interconnected objects. Information broadcast in a unidirectional manner, such as a television or radio broadcast, is not using cyberspace. Furthermore, manmade technologies that are not computers such as older televisions, radios, and telephones are not part of cyber. However, this line is blurring as new smart televisions and Voice over Internet Protocol phones are plugged into the network and become part of the physical infrastructure that bounds cyberspace. The definition further allows for the future development of biochip implants and other exotic microchip tools that can access networks.

Second, cyberspace is *truly unique* because while manmade technologies are required to enter and exploit all five domains, manmade technologies *govern* the interactions in cyberspace and *create* its geography.[35] The geography of cyberspace is made via the routers, switches, fiber optic cable, copper, and other linkages. These technologies are easily changeable and moved, making cyberspace a more fluid and dynamic domain than land, sea, air, or space. Since people create this aspect of cyberspace, people can duplicate and re-create it—unlike any of the other domains.[36] The mountains and valleys on land and the water in the oceans are much more difficult to change than the technologies creating cyberspace. If a link or path in cyberspace fails or is blocked, another link can be quickly created.

The final defining characteristic unique to cyberspace is how users manipulate its characteristics and properties to create, store, modify, change, and exploit information.[37] Using cyberspace is all about the information resident there, and operating in and through the domain to create and control information. This intangibleness of cyberspace, a

---

[33] "Merriam-Webster Dictionary," http://www.merriam-webster.com/dictionary/cyber (accessed 17 November 2012).
[34] "Dictionary.com," http://dictionary.reference.com/browse/cyber (accessed 17 November 2012).
[35] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 29; Rattray, "An Environmental Approach to Understanding Cyberpower," 256.
[36] J.B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (2011): 97.
[37] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

function and output of how people and organizations use it makes it more difficult to grasp conceptually than the other domains.

From these understandings of the proposed definitions of strategy and cyberspace, I can now describe the *purpose* of a cyberspace strategy. A cyberspace strategy should use cyberspace to "create advantages and influence events in all the operational domains and across the instruments of power to achieve the state's political objectives."[38] Using cyberspace is all about the information and the ability to manipulate perceptions of the strategic environment to your advantage.

Figure 2: JP 3-13 Definitions

Information Operations (IO): the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own

Computer Network Operations (CNO): the use of networked computers and supporting IT infrastructure systems by military and civilian organizations to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure

Electronic Warfare (EW): any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary

Source: Joint Publication 3-13, *Information Operations*, 13 February 2006, ix, II-4.

The electronic warfare mission in the DOD is divided into electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).[39] EA is the offensive portion of EW. Electronic warfare officers use electromagnetic energy, directed energy, or antiradiation weapons destroy enemy capabilities by attacking personnel, facilities, and equipment. Electronic protection is the defensive portion of EW. Electronic protection protects the EMS to ensure its availability for friendly use. An example of EP is the coordination and deconfliction of the use of the electromagnetic spectrum. Electronic warfare support includes actions that sustain both EA and EP. In support of EP, ES finds

[38] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 95.
[39] Joint Publication 3-13-1, *Electronic Warfare*, 25 January 2007, v.

sources of interfering electromagnetic energy in order to eliminate it. If the source cannot be eliminated, ES provides information on avoiding the threat.

Similarly, computer network operations (CNO), commonly referred to as cyberspace operations, is also broken down into three mission areas. The US DOD divides the CNO mission into computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE.) CNA consists of actions taken using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or to the computers and networks themselves. CND involves actions taken by computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. CND actions not only protect DOD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations. CNE includes enabling operations and intelligence collection capabilities conducted with computer networks to gather data from target or adversary automated information systems or networks.[40]

Cyberspace operations and EW are similar because of their use of the EMS. Military operators conduct EW in the EMS, while cyberspace operations take place within cyberspace, but uses electronics and the EMS. This shared use of the EMS in addition to the growth of wireless networks and the integration of computers and radio frequency communications has started to blur the line between what the military considers cyberspace operations and EW, and this effective blending has significant derogatory implications for cyber strategy and operations. EW may be used to set or support favorable conditions for cyberspace operations by enhancing networked sensors, denying wireless networks, or other related actions. In the defensive environment, EW systems may detect and defeat attacks across wireless access points. These actions are peripheral to cyberspace, and while extremely valuable, are not limited to or exclusively part of the cyber domain.

Cyberspace operations and EW are also similar because they are both considered core capabilities of information operations (IO). From Figure 2, IO is:

[40] Joint Publication 3-13, *Information Operations*, 13 February 2006.

"the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[41] Military operators use both EW and CNO to achieve the IO mission, but do so in their own ways. To accomplish the IO mission, operators conduct CNO by using computers and information technology (IT) systems, while EW is conducted using electromagnetic and directed energy. Although operators use CNO and EW as primary means to achieve the IO mission, IO is not their sole duty. As previously described, CNO and EW are distinct mission sets.

Cyberspace Superiority

Cyberspace superiority enables the relatively unimpeded use of cyber power. Cyberspace superiority is "the operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[42] This sets the expectation for some interference, but the idea of prohibitive interference is important because it does not say operations must be without *any* interference to be effective. Similar to the other domains, and considering the vastness of cyberspace, a military is most likely to have localized cyberspace superiority. Its ability to operate without excessive interference will be localized to a certain place for a certain amount of time. This concept of localized cyberspace superiority is very similar to Julian Corbett's idea of command of the sea, or sea superiority. Because the sea is so vast, its normal state is uncommanded, much like cyberspace.[43] Nonetheless, in support of operations in other domains, and for operations within its domain, sea and cyber command is possible—and necessary—when and where needed.

Some scholars argue that cyber superiority is not real, and even if it was, cyber operators could not attain it. Libicki asserts, "cyber superiority is a notional issue considering very few militaries use the cyber commons to do their serious work."[44] He

[41] Joint Publication 3-13, *Information Operations*, 13 February 2006, II-4.
[42] Air Force Doctrine Document 3-12, *Cyberspace Operations*, 30 November 2011.
[43] Julian Stafford Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 91.
[44] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 142 footnote 8.

does not expand much on this statement, but the US military is very dependent on the cyber commons. The numerous civilian contractors, who often work from outside a military facility, do important work for the military and are dependent upon the cyber commons for daily interactions. Furthermore, the US military executes its war-fighting generation mission on the unclassified network. In order to deploy troops the US must have localized cyber superiority to schedule the mobility aspect of its operation. Libicki further argues that since each side in a conflict has physical control over its own networks it is impossible for the other side to have superiority over it. The owners of the network simply have to remove the affected machines or deny access to a limited (secure) network thereby eliminating the ability of the other side to have superiority there. While this may be true, the network has been seriously degraded by the attack, and the machines taken off line are no longer functioning. The secure network is much more limited than the broader, open one where the attacker still operates. Indeed, the small amount of time the offensive side had access may have been all that was needed to carry out a successful attack or achieve the desired effects.

Cyber Attack, Cyber Power, and Cyber War

A cyber attack is one form of cyber operations and is defined as, "the deliberate disruption or corruption by one state of a system of interest to another state."[45] Preventing such attacks, or ameliorating their effects, amounts to the defensive form of cyber operations. As such, "Cyber operations take place in cyberspace and generate cyber power."[46] Cyber power is thus akin to the description of air power by the theorist William Mitchell, who called air power "the ability to do something in the air."[47] Similarly, cyber power is the ability to do something in cyberspace. When doing something in cyberspace is destructive, and met with counter-destruction in response, the resulting exchange of attacks between two *states* is a cyber war. Before exploring the idea of cyber war more fully, readers should understand what specifically constitutes a cyber attack, the attributes of cyber power that make a cyber attack possible, and finally some of the problems inherent with a cyber attack. From this understanding, I can explain the ideas behind a cyber war.

---

[45] Libicki, *Cyberdeterrence and Cyberwar*, 23.
[46] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 95.
[47] William Mitchell, *Winged Defense* (Tuscaloosa, AL: University of Alabama Press, 2009), 3-4.

The primary activity in cyberspace that does not constitute an attack is computer network exploitation (CNE). Computer network exploitation is espionage of a target system. The international community does not consider espionage an attack in laws of war and therefore it should not be in cyber.[48] The problem arises when a target perceives the use of CNE differently than the attacker intended. The target could easily believe pings on a firewall meant to precede CNE are actions preceding an attack.[49] Or, the state using CNE could make a mistake and disrupt a system, elevating its actions to an attack inadvertently. While CNE is not an attack, it does benefit from cyber power's inherent attributes just as an attack does.

The first inherent attribute of cyber power is that it is ubiquitous. This is quite apparent with the invention and widespread use of wireless and cellular technologies. People can access cyberspace from virtually anywhere and if there is a location people cannot access it, they can just build the infrastructure to extend cyberspace there. In addition to the virtually unlimited number of fronts in cyberspace, information is also able to move across vast distances nearly instantaneously.[50]

Cyber power's second inherent attribute is its unparalleled speed.[51] The movement of electromagnetic radiation eliminates the constraints of distance and time that are the classic limits on operations in the other domains. An attack may be executed on a target around the world in seconds—and be complete before the adversary's defense can respond. This attribute of cyber power enables Boyd's theory of war by providing leaders a way to increase or control the tempo of war to their advantage.[52] The spread of the Conficker worm in November 2008 highlights the speed of operations in cyberspace.[53] Within a month, it had infected 1.5 million computers in 195 countries, while some of the United States best security specialists were trying to contain it. By February 2009, experts estimated between ten to twelve billion computers were infected.

---

[48] Libicki, *Cyberdeterrence and Cyberwar*, 23-24.
[49] Libicki, *Cyberdeterrence and Cyberwar*, 24.
[50]Rattray, "An Environmental Approach to Understanding Cyberpower," 255.; Lambeth, "Airpower, Spacepower, and Cyberpower," 53.
[51] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 98.
[52] Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007), 235-36.
[53] Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011), 159.

Third, cyber power is deceptive. It is the ultimate weapon of deception because it can alter, subtract, or even add information in cyberspace to trick an adversary into believing something is true or deleting needed information so it does not know the information even exists.[54] This alters the perception of the adversary to make choices to the attacker's advantage that it otherwise would not make.[55] Part of cyber power's deceptive ability comes from its ubiquitous nature and that attacks can come from virtually anywhere. It is also deceptive because it is difficult for an attack victim to determine if a computer problem is a normal hardware or software error or an attack. In the air, land, and sea domain's it is clear if an attack has occurred because of the kinetic nature of an attack in these domains.

This leads to the fourth attribute of cyber power, its non-attributable nature.[56] Currently, because of an intended capacity for anonymity in the design and structure of much of cyberspace's hardware and software and a lag in the development of technology that can trace user malfeasance, it is time consuming and expensive to track a well-planned cyber attack to its source, if not sometimes impossible. Diplomatically, the problem with attribution is obtaining the cooperation of other states or owners of cyber hardware to share technical information to begin finding the source of the attack. However, this benefit to the attacker is likely to diminish with technology advancements and increasing public and private concern for increased security. In a DOD directed study, a research team found there are multiple ways to help resolve the attribution problem if money is invested in their development and deployment. Techniques such as network filtering, hardening routers and other hardware, and even changing the architecture of the Internet can help with attributing actions in cyberspace.[57] Although none of the methods offers a completely reliable solution, they offer more promise than current techniques.

---

[54] Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Burlington, MA: Butterworth-Heinemann, 2011), 41.
[55] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 103.
[56] Susan W. Brenner, *Cyberthreats : The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), 74.
[57] D.A. Wheeler and G.N. Larsen, "Techniques for Cyber Attack Attribution," (DTIC Document, 2003).

The fifth inherent attribute of cyber power is that it is inherently offensive (rather than defensive).[58] This attribute of cyber power derives from the summation of its first four attributes. While cyber power's inherently offensive nature highlights the ease of executing a cyber attack and creating effects, there are some problems worth highlighting.

The ability to coerce a state is one such problem with executing a cyber attack. Coercion can be broken down into two components: compellence and deterrence. A state compels another state by executing an undesired action and continuing that action until the target state responds in a desired manner. In cyberspace, a state would attack another in some way causing an adverse effect until the adversary state complied with its demands. Once the adversary responds in the desired way, the state will stop the attack.[59] To compel a state, the attacking state must announce both the activity and the reason for that action and the target state must understand the responses it must take to stop the activity. In cyberspace, compelling leaders of a state to take a certain action is difficult if leaders are not exactly sure how vulnerable their state is.[60] If they think they can withstand an attack, coercion probably will not work. Moreover, if the compelling state starts a coercive action at a level that does not hurt the adversary, it may lead the adversary to believe it can withstand any attack made. Another problem is announcing an action in cyberspace. Despite the fact that many leaders want to keep their cyberspace operations secretive, if they do announce an attack meant to compel a state and fail, they have now lost future credibility.

Some argue they have seen the difficulty with coercion in the Stuxnet cyber attack. They claim that after the attack on Iranian nuclear centrifuges, Iran did not stop its nuclear development program.[61] However, the attack in this case was not meant to be coercive. No state claimed the attack, nor did any announce what would have to happen to make further attacks or an escalation of attacks stop. A coercive attack must ensure the target state clearly knows what is at stake. Leaders used the attack in this case to create the effect of slowing Iran's nuclear development, which it did.

---

[58] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 98.
[59] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 72.
[60] Libicki, *Cyberdeterrence and Cyberwar*, 79.
[61] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 103.

The flip side of compellence is deterrence, and cyber power's inherent capabilities have made the deterrence of cyber attacks difficult to achieve. States achieve deterrence through a threat that prevents an adversary from taking an action for fear of the consequences. The deterring state must clearly state the action the target state must *not* take as well as what the consequences will be if the action occurs.[62] In order to deter an actor, a state must show it has the capability *and* will to respond if the undesired action happens, thereby making the threat credible.[63] In cyberspace, states often keep offensive capabilities secret, in great measure to maintain its deceptive attribute.[64] This in turn reduces the deterrent capability because the state's response capability is unknown. To eliminate this problem, some argue a state can use a non-cyber kinetic threat to deter cyber attacks. David Fidler argues against this claim stating a kinetic option for retaliation to a cyber attack is not proportional and does not follow the principles of *jus in bello*.[65] Unless the state is deterring against some large type of *physical* damage, this disproportional response causes the threat to lose credibility.

Additionally, cyber deterrence is made more difficult by the mass entry of single actors and small groups into cyberspace because of the low cost of entry. While it is possible to deter a nation-state, where attribution is verifiable and its physical presence vulnerable, it is much more difficult to deter non-state actors or groups.[66] With a nation-state there are things that can be held at risk, such as territory, population, or resources. However, single actors or groups might not feel they have anything to lose, nor do they necessarily have a physical space that leaders can hold at risk. Furthermore, because it is difficult to attribute an attack, an adversary has a high likelihood that the target would never be able to prove who conducted the attack, making deterrence very difficult. The other attributes of speed, ubiquity, and deception further compound the problem.

---

[62] Schelling, *Arms and Influence*, 70.
[63] Schelling, *Arms and Influence*, 35-54.
[64] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 93.
[65] David P. Fidler, "The Law of Armed Conflict and Cyber Conflict," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 76.
[66] Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," 100.

Until technologic and financial adaptations make significant inroads on attribution, leaders must tailor their deterrence to specific adversaries. This allows leaders to "influence the motives, cost-benefit calculations, and risk taking propensities."[67] Instead of only focusing on deterrence by imposing costs, they can consider denying benefits or offering incentives for adversary restraint.[68] Ultimately, the best method of deterrence in cyberspace may be defense, or perhaps futility is a better term, which works against *all* actors to eliminate the attribution problem. Making any attack futile will deny any benefit to an attacker regardless of who they are, or how fast and deceptive their form of attack is.[69] However, additional resources and technology would be required to enable this option, and any capacity to universally deny the capacity for obtaining benefits through attacking cyber (through strict control over access, impenetrable firewalls or crypto-security, or immediate proportional response, for example) potentially detracts from the benefits cyber supplies the intended users.

Furthermore, the possibility of escalation is a problem with using a cyber attack. Attacks in cyber space can grow or escalate, especially if the wrong state is attacked in retaliation due to the problems with attribution. Cyber-dependent states such as the United States have more to lose than states not dependent on cyber. Making this dependency worse, the United States is at least as vulnerable to attacks as other states, if not more so.[70] Libicki suggests, "The US may not want to legitimize retaliation because it is so vulnerable and has adequate conventional strength."[71] Instead of responding with a cyber counter attack, the US may simply want to use a conventional counter attack. However, responding with a conventional attack will only be likely in certain circumstances. The US would only want to use a conventional counter attack if the cyber attack created effects equivalent to those of a conventional attack. The effects will include the actual physical effect combined with the effect perceived by the state and its

---

[67] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 310.
[68] Kugler, "Deterrence of Cyber Attacks," 327.
[69] Jeffrey R. Cooper, "A New Framework for Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 113.
[70] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat To National Security and What To Do About It.* (New York: Ecco, 2010), 148.
[71] Libicki, *Cyberdeterrence and Cyberwar*, 28.

members. It is likely people will not perceive a cyber attack to be as damaging as a kinetic attack because it may not have the same psychological impact, due to cyberspace's virtual nature. Additionally, the US should only use a conventional response if it is willing to escalate the conflict. Regardless of the amount of damage of an instigating cyber attack, the adversarial state's leaders will most likely view a conventional response as an escalation towards war.

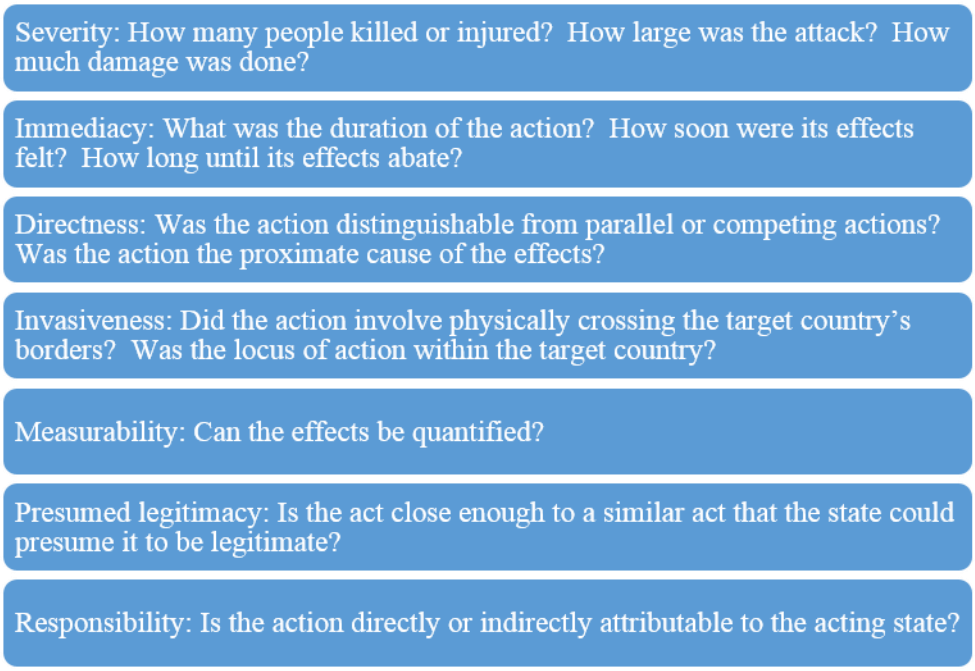
Along with the problems with using conventional force in response to a cyber attack, there can also be problems with the application of force *in* cyberspace. For example, attacks of force in cyberspace are likely to take the form of "attacks on a target's military and related systems [that] are usually meant to weaken the target's ability to respond to a crisis."[72] If a state attacks too far in advance it gives the target state time to recover by replacing affected systems and software. Taking an incremental approach to a cyber attack has the same problem. The target state is now aware of attacks, which allows it to improve its defenses and change the cyber landscape, making future attacks more difficult.

Another problem with cyber attacks is how to determine the threshold for calling a cyber operation an attack that meets the level of justified force in international law. To date, the international community has not agreed on a threshold, nor has the United States or China specified a unilateral threshold. The disadvantages are obvious. The international community is unlikely to agree on proper responses to an attack, and the time it takes to make a decision to retaliate—how, in what way, and how much—is made more difficult by not having policies in place. However, not making a specific threshold has the advantage of leaving decision room for the state based upon the context of the situation. In other words, the state's hands are not prematurely tied. This gives the state the ability to either take action or not and leaves the attacker with an unclear understanding of what the target will do. Thus, this gray area could aid in the deterrence of an attack.[73] To aid in working through this gray area, Naval War College Professor Michael Schmitt developed a quantitative scale covering seven factors that may be useful

[72] Libicki, *Cyberdeterrence and Cyberwar*, 82.
[73] Shelling discusses how the unpredictability of a situation adds to the danger of a crisis, thus aiding in deterrence. Schelling, *Arms and Influence*, 96-97.

in determining whether a cyber attack meets the threshold for lawful retaliation.[74] It is also useful in helping ensure minor attacks do not cause an escalation of the situation into something larger than it should be. The factors and questions associated with the factors are in Figure 3. Although Schmitt assigns a quantitative number to these items, there is still an element of judgment needed, leaving the answer based upon the perceptions of the decision makers and any biases they may have.

Figure 3: Factors to Consider for a Cyber Attack meeting Use of Force threshold



Source: Wingfield, "International Law and Information Operations," 527-30.

Given Schmitt's criteria, two basic schools of thought regarding the efficacy of cyber war occupy opposite sides of a spectrum. One school argues that cyber war is an empty threat and it really should not be worried about or focused on. The other school argues that cyber war is a very real threat and the consequences of a cyber war could wreak havoc by disabling militaries as well as shocking a civilian society's way of life. To place the relative import of cyber war along the scale of insignificance to global catastrophe, it is helpful to explain

[74] Thomas C. Wingfield, "International Law and Information Operations," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 527.

cyber war by looking at it divided into strategic and operational categories, which distinguish between the targets of cyber war.[75]

If cyber war is an empty threat, it does not deserve much attention. The first argument used is that the activities such as espionage, crime, most hacking, and breaches of intellectual property, while foreboding and a nuisance to society, do not meet the level of war. The validity of this argument is questionable, even though most scholars do not consider these activities, such as espionage, acts of war. They are excluded by definition. But this is a precarious position as "The difference between cyber crime, espionage, and attack or war is a couple of keystrokes."[76] A simple mistake could become an act of war. Moreover, the evaluation of crime and hacking meeting the threshold of war depends upon a decision by the state or the international community. If it is damaging to the state and it considers the action an act of war, then it is.

Others insist the problems discussed with cyber attack (e.g. non-attribution, deception, speed, etc.) are reasons there will *not* be a cyber war in the near future.[77] They also claim there has yet to be a cyber war despite the various cyber attacks on states.[78] Furthermore, Libicki argues that attacks on civilian infrastructure simply will not cause the societal problems others predict.[79] This argument is similar to the one Robert Pape makes against the use of strategic bombing by the US Air Force, claiming it simply does not work.[80]

On the contrary, simply because there has not been a cyber war does not mean there never will be. There are many reasons to believe there will be a cyber war, the

---

[75] Libicki, *Cyberdeterrence and Cyberwar*, 117, 39.
[76] Tom Gjelten, "Cyber Insecurity: U.S. Struggles To Confront Threat," *NPR*(2010), http://www.npr.org/templates/story/story.php?storyId=125578576 (accessed 26 April 2013).
[77] Tional James Andrew Lewis, "The Cyber War Has Not Begun," *Center for Strategic and International Studies*(2010), http://dev.csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf (accessed April 9 2013); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012); Libicki, *Cyberdeterrence and Cyberwar*. David L. Willson, "Cyberwar or Cyber Cold War?," *Information Systems Security Association Journal*(2012), http://www.titaninfosecuritygroup.com/UserFiles/HTMLEditor/Cyberwar%20or%20Cyber%20Cold%20War_ISSA0912.pdf (accessed 9 April 2013).
[78] Rid, "Cyber War Will Not Take Place."; Lewis, "The Cyber War Has Not Begun"; Willson, "Cyberwar or Cyber Cold War?".
[79] Libicki, *Cyberdeterrence and Cyberwar*, 137.
[80] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 314.

effects of which could be devastating to a country.[81] The highest form of cyber war is strategic cyber war or "a campaign of cyber attacks launched by one entity against a state and its society, primarily for the purpose of affecting the target state's behavior"[82] Such a strategic cyber campaign may already be under way. For example, one authority claims adversaries have already planted logic bombs in the US electrical infrastructure that could cripple it at any time.[83]

Cyber-dependent countries, including the United States, are the most vulnerable to a cyber attack and the effects of cyber power. An attack could be on any item of interest in cyberspace. US leaders consider cyberspace to be the nation's central nervous system, which qualifies it as a critical center of gravity for adversary targeting.[84] The nation's electrical power grid, financial institutions and transactions, communications links, production facilities, and military are all reliant upon cyberspace.[85] While the effects of an electrical outage may not be as painful to states that are much less dependent upon it (for example, North Korea), a long outage would cripple portions of the state's critical economic and war-fighting capacity. Prolonged outages in the United States would be more than an inconvenience. Civilian casualties due to temperature extremes, lack of timely weather warnings, and service delinquencies at hospitals and other care facilities would most likely cause civilian unrest. Citizens concerned with their savings could prompt a run on the banks, collapsing the entire financial industry. Adding to the enticement of an attack on the United States, most of this infrastructure is civilian owned and not protected by the DOD. General Keith Alexander, head of US Cyber Command, testified before the House Armed Services Committee's Subcommittee on Emerging Threats and capabilities in 2011 stating:

> "We believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are

---

[81] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*
[82] Libicki, *Cyberdeterrence and Cyberwar*, 115.
[83] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*, 59.
[84] Lambeth, "Airpower, Spacepower, and Cyberpower," 50.
[85] John A. McCarthy et al., "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, ed. F.D. Kramer, S.H. Starr, and L. Wentz (Washington, DC: Potomac Books Incorporated, 2009), 548-51.

> proliferating into national arsenals and possibly beyond … Segments of our nation's critical infrastructure are not prepared to handle this type of threat."[86]

With such extreme damage potential, coupled with the current difficulties with attribution in cyberspace, states with small conventional capabilities may be encouraged to use this asymmetric form of warfare.

Operational cyber war is considered more plausible than a systematic strategic effort to disable an adversary, even by those who do not believe a full-scale cyber war will happen. Libicki defines operational cyber war as "attacks against military targets and military-related civilian targets."[87] In this form of war, an adversary may simply attack to force the target to spend excessively on its defenses. US leaders and adversaries consider a key target of the US military to be the command and control over its forces, and while spending large sums to protect against continuous infiltration of its cyber operations, it has also caused it to become wary about reliance on the extremely efficient cyber capabilities it has developed. Today's militaries expect to operate in and through a cyber attack, and thus devote critical training to non-cyber redundant capabilities in case cyber attacks are successful. The usual information, such as GPS or data links, may have errant information added if it is available at all. Sheldon and other scholars believe the side that wins in a future war will be the side that can command and control its forces while deprived of information.[88] That may be so, but the expense of being able to do both cyber and non-cyber operations equally well is significantly greater than assuming cyber support will be unchallenged. Clearly, the US military not only believes cyber war is possible, it is preparing for it.

Summary

Although cyberspace is a relatively new war-fighting domain, it is critical that people learn about and understand it. Only after leaders and strategists thoroughly understand the benefits and drawbacks of cyberspace can they develop a strategy for it proper utilization. Cyberspace and cyber operations are not equivalent to communications, nor are they the same as EW. The definition I will use is "*the*

[86] J.C. Mulvenon and A.N.D. Yang, *The People's Liberation Army as Organization* (Santa Monica, CA: RAND Corporation, 2002), 5.
[87] Libicki, *Cyberdeterrence and Cyberwar*, 139.
[88] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 107.

proverbial ether within and through which electromagnetic radiation is propagated to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Cyberspace is similar to the other domains in that warfighters operate in and through it. It is distinct from the other domains because of its characterization, use of technology, manipulation of information, and significantly manmade nature. The manmade technologies govern the interactions in cyberspace and create its geography, while the natural portion of cyberspace, the EMS, characterizes the omnidirectional movement in cyberspace. Additionally, cyberspace is unique in how users use its characteristics and properties to create, store, modify, change, and exploit information.

The unique attributes of cyber power affect how users exploit cyberspace. Cyber power is ubiquitous, has unparalleled speed, is deceptive, highly non-attributable, and is offensive in nature. While cyber power adds some unique capabilities to the fight, it makes certain aspects of using cyberspace more difficult. It is more difficult to coerce a state in cyberspace than with conventional weapons in physical space. Compelling leaders of a state to take an action is difficult in cyber space as they may think they can withstand further attacks because they are unaware of their vulnerabilities, the initial cyber attack was not harmful enough, because states keep cyber capabilities secret, or the prospect of further harm is not believed. Deterrence is also difficult because it is hard to deter a state that can make an anonymous attack. Further, it is difficult to hold something of value at risk, such as land or people in physical space, and hold it at risk repeatedly. This currently makes denial the best form of deterrence in cyberspace. Additionally, problems with international and US law in determining the threshold of what is and is not a cyber attack is problematic. It leaves no boundary for potential adversaries and confuses a response to cyber incidents.

Ultimately, although it has yet to be proven, a cyber war could be very destructive to a state that is dependent upon cyberspace. Leaders who assume a cyber war will never happen and therefore decide not to plan for one are taking a tremendous risk and basing their decisions upon the hope it will never happen, in spite of the mounting evidence that cyber attacks are already occurring.

Chapter 2
China

In order to understand China's thoughts about cyberspace and its cyber strategy, it is important to understand China's view of the world, its strategic goals, and its overall military strategy. This provides the basis for understanding how cyber fits into its broader military strategy.

China's Strategic Goals

The interests of China and the threats it faces have been the catalyst in its development of strategic goals as well as its military goals and strategy. The principal strategic objectives are preserving communist party rule, sustaining economic growth and development, defending national sovereignty and territorial integrity, achieving national unification, maintaining internal stability, and securing China's status as a great power.[1] Some of China's key interests include natural resources, territorial disputes, economics, demographics, reunification with Taiwan, information security, and international concerns.[2] Furthermore, these interests are intertwined and drive each other. This interconnectedness creates the potential for a problem in one area of interest having a negative domino effect on the other interests.

China's need for resources is one of the primary catalysts driving its strategic goals and choices.[3] As China modernizes and grows its economy, it becomes increasingly dependent upon the import of natural resources and on foreign markets to access the resources. In 2008, China became the world's leading importer of crude oil and as of 2009 imported over 53 percent of its oil.[4] China's need for natural resources has driven many of the disputes with its neighbors.

The requirement for natural resources has resulted in disputes of ownership of the East China Sea and the South China Sea. "The East China sea contains approximately 7

[1] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," ed. Office of the Secretary of Defense (2012).
[2] "Annual Report to Congress: Military Power of the People's Republic of China 2009," ed. Office of the Secretary of Defense (2009), 3-9.
[3] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 3.
[4] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 3.

trillion cubic feet of natural gas and up to 100 billion barrels of oil."[5] Japan and China are disputing where to draw the line between the two, establishing ownership rights. In the South China Sea, China claims ownership of the Spratly and Paracel islands and their adjacent waterways. These waterways are the primary shipping lanes providing 80 percent of Japan, South Korea, and Taiwan's crude oil. These and other countries are disputing ownership of the islands and waterways.[6] The Chinese need for resources, which drive the territorial disputes, has a direct link to its economic development.

China's economic development and the reduction of the number of Chinese people in poverty has led to increased support for the communist party. This increased support underwrites its military power.[7] Any change or disruption in the improved economic situation could cause problems for the party and decrease the internal stability of the country. Furthermore, an economic disruption would slow China's plans for the mechanization and informationization of its forces.

The demographics of China are another potential source of internal stability. By 2000, 100 million people had migrated from the Chinese countryside to the industrialized urban areas, and an additional 400 million people are expected to migrate by 2030.[8] Additionally, the Chinese population is aging with the number of senior citizens almost doubling by 2025 according to US estimates, while the China National Committee on Aging estimates this will occur in 2053.[9] The stress of the movement of people on infrastructure as well as caring for an aging population will place significant pressure on the Chinese people, which may keep China somewhat internally focused.[10]

China has repeatedly stated its goal is the unification of China with Taiwan. China's leaders are currently focusing on keeping Taiwan from declaring its

---

[5] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 5.
[6] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 5; Jane Perlez, "China Sends Troops to Disputed Islands," *New York Times*(2012), http://www.nytimes.com/2012/07/24/world/asia/china-sends-troops-to-disputed-islands.html?_r=0 (accessed 10 April 2013).
[7] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 7.
[8] "Migration and Movement of People," http://www.chinaonlinecentre.org/china_people_migration html (accessed 10 April 2013); "Annual Report to Congress: Military Power of the People's Republic of China 2009," 7.
[9] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 7; "China's Aging Population to Double by 2053," *China Daily*(2012), http://usa.chinadaily.com.cn/china/2012-10/23/content_15837814 htm (accessed 10 April 2013).
[10] "Annual Report to Congress: Military Power of the People's Republic of China 2009," 7.

independence. With the United States committed to defend Taiwan from Chinese invasion, the goal of unification is secondary to the primary goal of stopping Taiwan from becoming an independent state. Chinese leaders hold the United States directly responsible for inhibiting unification and point toward the United States sales of weapons to Taiwan as the responsible party for "impairing peaceful development of cross-strait relations.[11]

In summary, a loss of resources would have a direct effect on China's ability to function as a modern country in the world market and would cripple its economic growth. A decrease in economic development could destabilize the country, in particular support for the communist party. The changing demographics are partially driven by the prosperity in the urban areas driving the move of people within China. This puts a tremendous strain on its infrastructure and economy, which would result in further spiraling instability. The problems with the unification of Taiwan put additional pressures on its economy as well as strain on relations with the international community.

China's Military Goals and Strategy

The four goals for China's military strategy are safeguarding national sovereignty, security, and interests of national development; accelerating the modernization of national defense and armed forces; maintaining social harmony and stability; and maintaining world peace and stability.[12] In support of these goals, the PLA has a strategy of active defense. In order to safeguard its sovereignty, security, and interests, China's military must guard against aggression and defend its territory including its interests in space, electromagnetic space, and cyber space. This includes the sovereignty of *claimed* territory, and China appears focused on opposing Taiwan's independence and asserting its claims on the Eastern and Southern seas. Chinese leaders feel Taiwan's quest for independence is the "biggest obstacle and threat to peaceful development of cross strait relations."[13] Their focus is also on stopping the separatist movements for Turkistan and Tibet's independence.

[11] "China's National Defense 2010," Information Office of the State Counsel of the People's Republic of China, http://www.china.org.cn/government/whitepaper/node_7114675.htm (accessed December 15 2012).
[12] "China's National Defense 2010," II.
[13] "China's National Defense 2010," I.

To accelerate and modernize its national defense and armed forces the primary goal is to "achieve mechanization and major progress in informationization by 2010."[14] China is working hard to modernize its armed forces and strengthen its strategic planning. The goal is to upgrade armed forces quality while downsizing its size. As proof of China's commitment to informationization, in 2000 its electronic warfare technologies were from the 1950s-1980s. By 2006, the Chinese had "technological parity with or superiority over most potential adversaries."[15]

To maintain social harmony and stability the Chinese armed forces participate in humanitarian efforts following their tenet of serving the Chinese people.[16] To maintain world peace and stability Chinese leaders declare they uphold the security concepts of "mutual trust, mutual benefit, equality and coordination, peaceful settlement of disputes, opposes the use of force at will, opposes acts of aggression and expansion, and opposes hegemony and power politics."[17] China's declared military strategy supports its aim of maintaining peace and stability.

China's declared military strategy is active defense. The Chinese concept of active defense includes changing to offensive operations under favorable conditions to exploit vulnerabilities and gain the initiative.[18] This strategy appears to say China will not attack unless first attacked by another state. Then, in a Sun Tzu style of warfare, it will wait to go on the counteroffensive when the best opportunity for seizing the initiative presents itself.[19] However, its view of information warfare differs from their overarching strategy of active defense. Understanding the Chinese view of cyberspace and cyber war, which combines electronic and cyber warfare, will explain this differentiation.

China and Cyberspace

The Chinese do not specifically talk about cyberspace. They view the war-fighting dimensions as land, sea, air, space, and the information sphere.[20] Of note,

[14] "China's National Defense 2010," II.
[15] "Annual Report to Congress: Military Power of the People's Republic of China 2009," VIII.
[16] "China's National Defense 2010," II.
[17] "China's National Defense 2010," II.
[18] "China's National Defense 2010," II.
[19] Sun Tzu, *The Illustrated Art of War* (New York: Oxford University Press, 2005), 128.
[20] Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *PLA Academy of Miliary Science and the China Military Science Association* (2002). Although the Chinese do not refer to the fifth domain as cyberspace, some sources state the Chinese believe the fifth domain is the electromagnetic

information operations are becoming the predominant concept in warfare for China. Its military doctrine supports this as it has shifted from a "people's war under modern conditions to limited local war to limited war under high tech conditions."[21] Furthermore, the former director of the PLA's Communications Department, Major General Dai Qingmin has written multiple articles declaring that information is everywhere and will play "an increasingly vital and prominent role in a war…serving as a basis of force for a war."[22] He also states a war in physical space is likely to become a war in information space.[23] Additionally, the Chinese believe future combat operations will have information as the center of gravity and achieving information superiority will be required before attaining air, sea, or space superiority.[24]

The Chinese view information operations as made up of six forms: operational security, military deception, psychological warfare, electronic warfare, computer network warfare, and physical destruction.[25] The primary difference between the United States and China's views of information operations is in the latter's stress of the use of EW and cyber operations, which it considers the main components of information warfare. The Chinese emphasize how these two elements must work together in combined operations. Military operators must use cyber operations and EW together because the information is obtained and transmitted in the EMS and processed or utilized in a computer network. "Electronic war is bound to focus on sabotaging information gathering or transmission whereas a network war (cyber war) is bound to focus on sabotaging information processing or utilization."[26]

The distinction between China's and the United States' view of cyberspace is small, but relevant. While the United States views cyberspace as the space created by both manmade components and the naturally existing electromagnetic spectrum, the Chinese do not refer specifically to cyberspace. They see the space where the

---

domain. Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 16.

[21] "Country Report: China," *The Economist*, no. 2 (2012).

[22] Dai Qingmin, "Innovating and Developing Views on Information Operations," *China Military Science* (2000).

[23] Qingmin, "Innovating and Developing Views on Information Operations."

[24] Qingmin, "On Integrating Network Warfare and Electronic Warfare."; Mulvenon and Yang, *The People's Liberation Army as Organization*.

[25] Qingmin, "On Integrating Network Warfare and Electronic Warfare."

[26] Qingmin, "Innovating and Developing Views on Information Operations."

information travels as electromagnetic space, where EW occurs. Militaries execute a network war to sabotage the information processing or utilization of a computer. Network war and EW are inseparably entangled because the information must cross the electromagnetic space when traveling from computer to computer. Dai Qingmin claims, "A network war could not be launched without electronic fighting means."[27] The Chinese have titled this strategy, which merges EW and CNA, Integrated Network Electronic Warfare (INEW).

The Chinese have associated several characteristics with INEW. Integrated network electronic warfare has comprehensive combat objectives and increases the effectiveness of combat operations. Information systems and computer networks have become the "lifeblood of nations' economies and the nerve center of armed forces."[28] Attacking these vital targets can weaken and paralyze the enemy's diplomatic, economic, and military war making capabilities. The integrated nature of INEW increases the effectiveness of combat operations. By cutting the nerves of the enemy, INEW paralyzes the enemy. Thus, the effects are greater than any traditional or single form of combat operations. The Chinese also recognize the ubiquitous quality of cyberspace and the electromagnetic spectrum, and further state they can conduct integrated network electronic warfare "anywhere networks and electromagnetic waves reach."[29]

To carry out the operation of paralyzing the enemy before other combined operations commence, Chinese literature suggests preemptive attacks are necessary. In particular, Dai Qingmin has advocated for the use of preemptive attacks to achieve information superiority.[30] To prepare for these attacks, he recommends cyber warfare units infiltrate the target's networks during peacetime.[31] Authors of the PLA's *Information Confrontation Theory* also recommend this strategy, calling for cyber forces

---

[27] D. Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare." *Journal of Defence Studies* 4 (2010): 38-39.
[28] Qingmin, "On Integrating Network Warfare and Electronic Warfare."
[29] Qingmin, "On Integrating Network Warfare and Electronic Warfare."
[30] Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare."; Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 9.
[31] Timothy Lloyd Thomas, *Dragon bytes: Chinese Information-War Theory and Practice from 1995-2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 128; Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 9.

to plant malicious software that will remain inactive and hidden until needed or some predetermined time. This preemptive strategy seems to contradict the Chinese longstanding declaration of active defense, but appears logical considering their views of how to use INEW.

China's Cyber Capabilities and Displays of the PLA's Military Strategy

Although the Chinese combine CNO and EW into their strategy, I will primarily examine China's CNO capabilities to focus on determining the effectiveness of a first-strike stratagem in cyberspace. Limiting the scope also allows for a better comparison to the US, which tends to keep CNO and EW as distinct operations. However, because the Chinese view CNO and EW as an integrated operation, limiting the scope to strictly cyber operations is not completely feasible. The capabilities are China's means to execute its strategy. To understand these capabilities I will look at how the PLA has organized its cyber operations as well as its human resources and technical capabilities. Examining China's recent military exercises is one of the best ways to show how developed its technical capabilities are. These exercises have a second and equally important benefit, which is proving the existence of its INEW strategy and how the PLA would employ it.

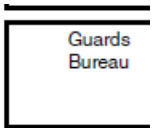
The PLA has divided its General Staff into four departments. The Third and Fourth Departments are responsible for cyber operations and EW.[32] Neither the PLA nor other authors have published very much in unclassified open source documents about the number of personnel in each division—or even about the divisions themselves.[33] What has been published suggests both the PLA's adaptation to the INEW strategy as well as its importance. The Third Department appears to be responsible for signals intelligence collection and analysis, CNE, and CND.[34] The Third Division is responsible for "overseeing one of the largest and most sophisticated SIGINT and cyber collection infrastructures in the world and certainly the most extensive in the Asia-Pacific region."[35]

---

[32] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 44-46; "Chinese Intelligence Agencies," Global Security, http://www.globalsecurity.org/intell/world/china/index html (accessed 27 April 2013).
[33] Mulvenon and Yang, *The People's Liberation Army as Organization*, 167.
[34] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 44.
[35] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 46.

Based upon the importance the PLA places on the need for CNE to prepare and conduct CNO as well as using INEW in advance of physical military operations, these departments are particularly important. [36] The PLA established the Fourth Department, which is responsible for CNO and EW, in 1990.[37] Various authors believe this division adopted the INEW strategy when the PLA named Dai Qingmin the department's head based upon his various publications advocating the strategy.

Figure 4: General Staff Department of the Peoples' Liberation Army



Source: Mulvenon and Yang, *The People's Liberation Army as Organization*, 129.

China has developed a high-tech militia to supplement the PLA's CNO and EW capabilities. China began recruiting its militia around 2002, but made it a priority in its 2006 National Defense whitepaper stating the priority was to recruit members with high-tech backgrounds in all services. To accomplish this, the Chinese would shift from

[36] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 19.
[37] I.C. Smith and N. West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD: Scarecrow Press Incorporated, 2012), 95.

recruiting in rural areas to the high-tech urban areas.[38] Since the start of this effort, China has utilized this high-tech militia by establishing information warfare units to develop viruses to attack enemy computer systems and networks as well as methods to protect its own systems and networks. [39] These units have the ability to plant information mines, conduct information reconnaissance, change network data, release information bombs, dump garbage information, disseminate propaganda, apply information deception, release clone information, organize information defense, and establish network spy stations.[40] With the almost unlimited work force combined with these offensive and defensive capabilities, the militia provides the PLA with a formidable means for conducting a cyber war. However, the command and control structure of these militia units remains unclear.

The Chinese government has built a network infrastructure that is technologically advanced and that provides protection from foreign espionage and cyber attack. First, the infrastructure is primarily fiber optics with satellite short-wave communications as its secondary means.[41] Unlike copper cabling, which external actors can access via common signals or electronic intelligence collection methods, external actors must physically tap fiber optic cabling to gain access to collect information. This makes cyber espionage on China's network more difficult than a country whose network has copper cabling. Second, China's firewall provides it the capability to disconnect the nation's networks from cyberspace if necessary. This ability provides the Chinese a distinct advantage to defend against a cyber war or in preparation of one.[42]

During June 2011, an article noted that the PLA has integrated INEW tools into a PLA fires unit for support.[43] This allows various units to employ EM jamming and CNA in support of individual units and provides the units a level of integration beyond what

[38] "China's National Defense 2006," Information Office of the State Counsel, http://www.china.org.cn/english/features/book/194421.htm (accessed January 21 2013).
[39] Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare." "Annual Report to Congress: Military Power of the People's Republic of China 2009."
[40] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*, 57-58.
[41] "China's National Defense 2010," III.
[42] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*, 148.
[43] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 23.

the PLA could be achieve by keeping INEW assets at the division level and provides the capability for missions at all levels of conflict.[44]

China's military and commercial cyber capabilities are closely integrated. Using national-level grants, China has invested in at least 50 civilian universities to conduct information security research to augment military research.[45] The quality of the research the universities are conducting is on the leading edge as shown through the development of the world's fastest supercomputer in 2010.[46] This type of development is in line with China's published goal of a rapid modernization of its military as well as the government's dual use of the information technology sector to assist the PLA. Krekel *et al* best summarized this integration of civilian and military capabilities, "Taken in the aggregate, recent developments in Chinese CNO applications and R&D point to a nation fully engaged in leveraging all available resources to create a diverse, technically advanced ability to operate in cyberspace as another means of meeting military and civilian goals for national development." [47]

The PLA's actions have proven its desire to integrate INEW into combat operations as well as achieve information dominance at the beginning of conflict. During a 2004 exercise, a unit within the PLA reportedly used CNA to penetrate the adversary's command and control network minutes after the exercise started. This particular unit has steadily informationized by upgrading and renovating its equipment. Additionally, the unit has focused on training its members with the report stating, "Through training, thus far, all the cadres and nearly 50 percent of the troops at this unit have passed state computer examinations and this unit has noticeably upgraded its troops' scientific and technological qualities."[48]

Multiple PLA exercises display the PLA's capabilities as well as how the PLA is focusing on integrating information warfare into its kinetic operations with the

---

[44] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 23.
[45] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 9.
[46] Manikandan Raman, "China Makes World's Fastest Supercomputer," *International Business Times* 28(2010), http://www.ibtimes.com/china-makes-worlds-fastest-supercomputer-246732# (accessed 27 April 2013).
[47] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 108-09.
[48] "Highlights: Chinese PLA's Recent Military Training Activities ", *FBIS Report* (2004).

employment of its INEW strategy. The use of INEW at the beginning of the exercises to affect adversary command and control further illustrates the shift from an active defense to a preemptive strategy. The PLA used INEW during Exercise Leap Forward 2009 and Exercise Iron-Fist 2009.[49] Information confrontation was one of the eight evaluated areas in the training. This focus on information operations supports the PLA's goal to integrate INEW into its combined operations.[50] Additionally, during Exercise Friendship 2010, the blue force PLA units coordinated an attack to degrade red force's information command networks at the start of the exercise. These actions further confirm the PLAs desire to gain information dominance at the beginning of a conflict.[51]

During Exercise Mission Action 2010, the PLA showed its progress in executing large-scale joint operations using INEW. The PLA successfully degraded enemy command and control systems using computer network attacks.[52] Assistant Chief of Staff Chen Yong and Assistant Director Wei Liang of the General Political Department lauded the results of the exercise: "For the first time, communications and electronic countermeasures as well as network confrontation were carried out throughout the exercise in all stages and all actions, indicating that a new model was created for organizing information system-based system-to-system confrontation drills."[53]

Although the PLA is continuing to increase military investment, exercise its information warfare capabilities, and stress informationization, a senior officer within the PLA states there are still problems to overcome, despite Chinese and Western media's

---

[49] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 21; "'Iron Fist-2009' military exercise in Jinan MAC ", *PLA Daily*(2009), http://china-defense.blogspot.com/2009/11/iron-fist-2009-military-exercise-in html (accessed 27 April 2013).

[50] Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." DTIC Document, 2009, 17; Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 21.

[51] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 21.

[52] "China PLA 'Mission Operations 2010A' military exercise started," http://www.chinamilitary net/china-pla-mission-operations-2010a-military-exercise-started.html (accessed 27 April 2013); Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 19.

[53] "Majestic and Powerful Forces, Fierce and Sweeping Actions Over a Thousand Miles -- Review of, and Thoughts About, the 'Mission Action-2010C' Trans-region Mobile Exercise," *Chengdu Zhanqi Bao*(2010), https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_0_0_43/content/Display/22118627?returnFrame=true (accessed 10 November 2010). OSC ID CPP20101222478002

portrayal of PLA operational success in these various training objectives.[54] On September 27, 2011, Chen Weizhan, head of the Military Training and Service Arms Department of the Guangzhou Military Region, stated informationization was still in its infancy and various generations of technology are in concurrent use. This variation in technology has led to compatibility issues between various units, negatively affecting combined training.[55] Thus, despite the progress the PLA has made in its information warfare capabilities, it still has some problems and issues to resolve.

US Views of Cyberspace Activities Attributed to China

There have been various activities in cyberspace attributed to China in the last 10 years. While the media has labeled some of these activities as an attack, many of them fall under the realm of crime or CNE. As previously discussed, there is a gray area between what CNE is and what elevates it to an attack, with the strategic difference being the intent of the attacker and the tactical difference consisting of only a few keystrokes. Further blurring this line is the use of CNE in the conduct of an attack. For the more advanced attacks, the attacker must know the architecture of cyberspace and will use CNE to prepare. China has specifically noted the need for using CNE in preparation of an attack.[56] Figure 5 shows a depiction of Chinese activities according to the US-China Economic and Security Review Commission. This figure shows the frequency of and target of China's alleged activities.

Security analysts see China's attacks increasing in sophistication as well as intensity. Richard Bejtlich, chief security officer for the cyber-security firm Mandiant states, "They remain aggressive—they are kicked out one day and try to get back in the next day."[57] Along with the intensity of attacks, the hackers are going after software weaknesses instead of duping employees through spear fishing techniques. Of the two attack vectors, the former is more difficult than the latter. The US-China Economic and

---

[54] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 21.
[55] Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 22.
[56] Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare."; Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 9.
[57] Lolita C. Baldor, "Chinese Cyber Attacks On U.S. Continue Totally Unabated, Leon Panetta," *Huffington Post*(2012), http://www huffingtonpost.com/2012/09/20/chinese-cyber-attacks-leon-panetta_n_1899168 html (accessed 23 January 2013).

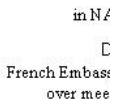
Security Review Commission stated, "The volume of exploitation attempts yielded enough successful breaches to make China the most threatening actor in cyberspace." As of December 6, 2012, the US intelligence committee is trying to determine the cost of these exploitation attempts to the United States.

Senior leaders in the US recognize the growing threat of China's activities in cyberspace. General Alexander, head of the US National Security Agency and US Cyber Command, acknowledged "a 17-fold increase in computer attacks on American infrastructure from 2009-2011."[58] Although these attacks are not all attributed to China, Republican Representative Michael McCaul, Chairman of the subcommittee on Oversight, Investigations, and Management, believes "China's cyber warfare capabilities and the espionage campaigns are the most prevalent of any nation state actor."[59] Their actions include lacing the United States infrastructure with logic bombs. While there is no clear unclassified listing of the specific infrastructure, it could include things such as electric grids, water supplies, computer and cell phone networks, and banking infrastructure. Although they have not gone off yet, military and civilian leaders believe these logic bombs are a clear threat to the United States security.

[58] "Cyberattacks on critical infrastructure increase 17-fold, says NSA chief," *Infosecurity-magazine*(2012), http://www.infosecurity-magazine.com/view/27275/cyberattacks-on-critical-infrastructure-increase-17fold-says-nsa-chief/ (accessed 23 January 2013).

[59] Homeland Security Subcommittee: Oversight and Management Efficiency, *America is Under Cyber Attack: Why Urgent Action is Needed*, 24 April 2012. In further congressional testimony, it is also noted that China is conducting CAN and CNE operations. House Committee on Foreign Affairs, *China's Quest for a Superpower Military*, 2007.

Figure 5: Timeline of Significant Chinese-related Cyber events from 1999-2009



Source: Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 67.

Summary

In summary, China's key interests are closely linked to its strategic objectives of preserving communist party rule, sustaining economic growth and development, defending national sovereignty and territorial integrity, achieving national unification, maintaining internal stability, and securing China's status as a great power.[60] Due to the interconnected nature of its interests, a setback in one area could cause setbacks in others. A loss of resources would have a direct effect on China's ability to function as a modern country in the world market and would cripple its economic growth. A decrease in economic development could destabilize the country, in particular support for the communist party. The prospect of prosperity in the urban areas has encouraged the Chinese people to move from rural China to more urban areas, changing China's demographics. The destabilizing effect of this shift in demographics could affect the party as well as put a tremendous strain on their infrastructure and economy, which would result in a downward spiral of instability. The problems with the unification of Taiwan put a strain on its economy as well as relations with the international community, of which the United States is its second largest trading partner, following the European Union.[61]

To meet the state's strategic aims, China's military strategy aims to safeguard national sovereignty, security, and interests of national development; accelerate the modernization of national defense and armed forces; maintain social harmony and stability; and maintain world peace and stability. The strategic aim to unify with Taiwan is at the heart of their aim to safeguard national sovereignty, but also includes space, electromagnetic space, and cyberspace. The Chinese have been working to achieve mechanization and informationization of its forces for modernization, although the Chinese are attaining their aggressive goal of military modernization while simultaneously declaring they oppose acts of aggression and expansion as well as hegemony and power politics. While this makes one question Chinese leaders' motives,

[60] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012."
[61] "European Commission Trade: China," European Commission, http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/china/ (accessed 23 March 2013).

the PLA's declaration of a strategy of active defense makes their actions appear slightly less aggressive.

The Chinese view of cyberspace and cyber operations is different from the United States. They see EW and cyber operations intertwined because operators obtain and transmit information in the EMS and then process and use it in a computer network. This view gives their EW and cyber operations a form of synergy not possessed if seen as completely separate operations. The Chinese also emphasize the importance of these networks as the "lifeblood of nations' economies and the nerve center of armed forces."[62] Furthermore, Chinese leaders have advocated for preemptive attacks to achieve information superiority, even going as far as recommending the infiltration of adversarial networks during peacetime.[63]

China's organization and activities in cyberspace emphasize its shift towards the INEW strategy and its use early in a conflict. The PLA has combined its EW and cyber operations into the 4th Division under Dai Qingmin, who first advocated the INEW stratagem. His leadership further proves adoption of this strategy. Additionally, in recent exercises the PLA has shown its use of INEW to attack an adversary's command and control networks preemptively to attain an advantage. These exercises and the continued activities in cyberspace targeted at the United States emphasizes the PLA as a growing threat to peace in cyberspace.

[62] Qingmin, "On Integrating Network Warfare and Electronic Warfare."
[63] Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare."; Krekel, Adams, and Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 9.

Chapter 3
United States

In contrast to deriving China's strategy for cyberspace from various military leaders' writings, the United States has published several documents that are a start at outlining its goals in cyberspace. From an understanding of US strategic and military goals, I can later evaluate the utility of a first-strike stratagem in accomplishing them. Furthermore, by understanding the declared US cyber strategy and understanding the United States' cyber capabilities, I can determine how first-strike fits and what is and is not possible with respect to a first-strike stratagem.

United States' Strategic Goals

The United States' four primary strategic goals of security, prosperity, values, and international order are outlined in the 2010 National Security Strategy (NSS).[1] The first goal is "the security of the United States, its citizens, and US allies and partners. The second goal is a strong, innovative, and growing US economy in an open international economic system that promotes opportunity and prosperity. The third goal is respect for universal values at home and around the world. Finally, the US desires an international order that promotes peace, security, and opportunity through stronger cooperation to meet global challenges."[2] A look at each of these goals in depth will help in the later analysis (in Chapter 5) of whether or not a first-strike in cyberspace stratagem will assist in achieving these aims.

The 2010 NSS reveals several focus areas to achieve the security of the United States, its citizens, and US allies and partners. The US can improve the security of the state and its citizens by focusing on bolstering its current security measures regarding the nation's vital infrastructure as well as improving its resilience to changing conditions or interruptions. It can improve the security of the state and its allies by continuing to disrupt, dismantle, and defeat Al-Qa'ida and its violent extremist affiliates around the world. In coordination with this goal, the NSS states, "The American people face no

[1] The following section is a summary of the NSS. Barack Obama, "National Security Strategy," (Washington DC2010).
[2] Obama, "National Security Strategy," 17.

greater or more urgent danger than a terrorist attack with a nuclear weapon," calling for a reversal in the spread of nuclear and biological weapons.[3] Another threat to the US national security, as well as public safety and the economy, is the threat from cyberspace. In order to secure cyberspace, the United States plans to invest in people and technology to protect critical government networks and improve the resilience of networks to recover from attacks quickly. It also plans to strengthen partnerships and work on international issues such as laws for cybercrime and an agreed upon appropriate response to cyber incidents.[4]

To work towards the goal of a prosperous United States the NSS outlines several areas it will focus on to achieve this goal.[5] The United States will strengthen its education programs as well as its human capital. It will work to improve access to higher education as well as the quality of the education, focusing on science, technology, engineering and math to produce critical thinkers and promote innovation. The impacts of these will help achieve the second area of enhancing science, technology, and innovation. In particular, the military will use this technology to defend the United States. The United States plans to achieve balanced and sustainable growth by saving and exporting more and opening foreign markets to its products and services. It will also accelerate sustainable development in emerging economies by investing in development to help narrow inequality and expand state capacity.

The third strategic goal listed in the NSS explains is the promotion of universal values abroad. United States leaders believe these values are "an individual's freedom to speak their mind, assemble without fear, worship as they please, and choose their own leaders; they also include dignity, tolerance, and equality among all people, and the fair and equitable administration of justice."[6] US leaders believe in the expansion of these rights because "governments that respect these values are more just, peaceful, and legitimate."[7] In order to promote these values, US leaders feel the best way is by setting the example.

---

[3] Obama, "National Security Strategy," 23.
[4] Obama, "National Security Strategy," 28.
[5] Obama, "National Security Strategy," 28-35.
[6] Obama, "National Security Strategy," 35.
[7] Obama, "National Security Strategy," 37.

The NSS final strategic goal is straightforward. The United States leaders desire a just and sustainable international order to handle common challenges cooperatively. To achieve this goal they plan to build upon alliances as well as other leading centers of influence. Concerning China, the NSS particularly states US leaders plan to focus on regional stability with a focus on China's relationship with Taiwan, human rights, weapons of mass destruction proliferation, and climate change.[8] As a warning to China, it also states American intentions of monitoring China's military modernization to ensure it is not out of tune with US interests, while at the same time encouraging China to make choices that will contribute to international peace and security.[9] To further cooperation, the NSS states the American leaders will work to strengthen institutions, such as the United Nations, and shift economic focus to the G-20. Finally, US leaders desire to make significant progress on global challenges through cooperation. These challenges include climate change, infectious disease, transnational crime, and safeguarding the global commons. The NSS specifically discusses the importance of cyberspace and the need for norms of behavior in the international community.[10]

The American's goals are divided between focusing on the security and prosperity of the country and its people and focusing on fostering a cooperative international community to handle problems together. Within the context of its security, American leaders specifically pointed out their right to use military force in its defense.[11] Although the NSS referred to multiple regions, for this essay it is important to note the tone used as a warning to China. Although US leaders are welcoming China to participate in the international community and act responsibly, they will be watching China's military developments to ensure it is not threatening the United States and its interests.

United States' Military Goals and Strategy

The US DOD National Military Strategy (NMS) was developed as the military aspect to help achieve the goals outlined in the NSS.[12] The goals in the NMS are to counter violent extremism, deter and defeat aggression, strengthen international and

[8] Obama, "National Security Strategy," 43.
[9] Obama, "National Security Strategy," 43.
[10] Obama, "National Security Strategy," 50.
[11] Obama, "National Security Strategy," 22.
[12] The following section is a summary of the NMS. "National Military Strategy," ed. Department of Defense (2011).

regional security, and shape the future military force. The military's protection and use of cyberspace helps achieve all of these aims. Understanding these aims will also aid in evaluating whether a first-strike stratagem in cyberspace will help achieve these aims with respect to China (in Chapter 5).

The US military plans to counter violent extremism because it threatens the security of the American people, its territory, and its way of life. The military plans to reach this goal by eroding the legitimacy of terrorist organizations and those supporting them. In concert with the other instruments of power, the military will use force when directed to achieve the nation's ends, but stresses force will be consistent with American values and international law.

The military plans to accomplish its goals through a combination of deterring and defeating aggression. Following the NSS's first strategic goal, the military plans to deter the use of nuclear weapons by advancing Ballistic Missile Defense capabilities. It also plans to focus on deterring WMD proliferation because the threat to American security as well as the security of other states. Furthermore, the military plans to enhance deterrence in cyberspace by developing the capability to fight through a degraded environment as well as improving its ability to attribute attacks in cyber to their source.[13] To defeat aggression, and to preserve peace and security, the US military plans to defend the country and its allies as necessary. The US strategy emphasizes the importance of space and cyberspace in its ability to act offensively. Part of the military's strategy to ensure access to these domains includes responses across the spectrum of options. In the NMD, military leaders recognize and call attention for the need to develop authorities to make action in cyberspace effective. The other border area making US operations in cyberspace difficult are highlighted in the third goal.[14]

To achieve the goal of strengthening international and regional security, the military plans to work with international partners as well as other agencies within the United States. Concerning cyberspace, the military plans to work with the Department of Homeland Security to improve domain awareness to help security the nation's critical

[13] "National Military Strategy," 7-8.
[14] "National Military Strategy," 9-10.

infrastructure.[15] The NMS discusses the various regions around the world and ends with a focus on China. The military hopes to develop a "military-to-military relationship with China" with the goal of reducing misperceptions and miscalculations.[16] Following the concern expressed in the NSS about China's military modernization, military leaders echo concern about China's strategic intent as well as its assertive actions in space, cyberspace, the Yellow Sea, East China Sea, and South China Sea. This concern is followed by a statement aimed at deterring China's aggressive actions stating military leaders have the will and ability to counter actions that threaten the nation's security or its use of cyberspace.[17]

Finally, military leaders plan to achieve all these and future goals by shaping the future force. By providing military members the right types of training, and investing in needed technologies, the military will have the capability and readiness to deter and respond to threats. While leaders will remain focused on protecting all domains, concerning cyberspace the military will protect its networks through a resilient architecture that can recover from attacks using detection, deterrence, denial, and defense in depth.[18]

United States' Cyber Strategy

Very recently, the United States' leaders have published a couple of documents that are the preliminary outlines of a strategy for cyberspace at the grand strategic and strategic levels. President Obama published the United States International Strategy for Cyberspace in 2011. In it he outlines the desired future for cyberspace as well as the United States' role in achieving that future. He follows this by explaining seven policy priorities he has in achieving this future. Also in 2011, the United States DOD published the second document, which is its strategy for operating in cyberspace. Military leaders explain five strategic initiatives guiding their strategy for operating in cyberspace.

The United States President clearly outlined the goal for the future of cyberspace. The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international

[15] "National Military Strategy," 11-12.
[16] "National Military Strategy," 14.
[17] "National Military Strategy," 14.
[18] "National Military Strategy," 19.

trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[19] United States leaders desire end-to-end openness and interoperability. If it is not interoperable, then the various proprietary objects will segment cyberspace by denying access to large portions of the world's population. This could quickly increase the divide between the states that currently have the technology and those that do not.[20] They also desire the data to be secure in transit as well as in storage and that delivery of data be reliable. The United States can improve security by reducing vulnerabilities with technical standards and solutions and a secure supply chain. Additionally, establishing global norms for cyberspace can help achieve openness, interoperability, security, and reliability.

From the desired future of cyberspace, US leaders envision three primary ways the United States can play a role. By using diplomacy and strengthening government partnerships, United States leaders hope to build a consolidated effort towards their vision of cyberspace. Second, the United States will develop plans to defend its networks by focusing on increasing network resilience to limit the effects of attacks.[21] Furthermore, the ideas for deterrence mirror the statements made in the NSS explaining the need for norms on responses to attacks as well the United States' right to respond to attacks through a variety of means including diplomatic, informational, military, and economic.[22] Finally, the United States plans to focus on development in the areas of technical expertise, cyber security, and policy.

The International Strategy for Cyberspace comprehensively explains seven policy priorities the United States will work to achieve. These priorities will help the United States along with its allies and partners develop and sustain open, interoperable, secure and reliable use of cyberspace. Figure 6 is an outline of the policy priorities, which all

---

[19] Barack Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," (2011), 8.
[20] Peter Dicken, *Global Shift: Mapping the Changing Contours of the World Economy*, 6th ed. (New York: Guilford Press, 2011), 476.
[21] Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 13.
[22] Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 14.

have elements of the US' envisioned role using diplomacy, defense, and development to achieve its desired future.

Figure 6: Seven Policy Priorities for the International Strategy for Cyberspace

Source: Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 17-24.

While the International Strategy for Cyberspace creates a grand strategic picture for the United States, the military portion is explained in the Department of Defense Strategy for Operating in Cyberspace.[23] This strategy is broken down into five strategic initiatives and links to the grand strategy by accomplishing these initiatives with defense, diplomacy and partnership building, as well as developing the force and technology. The overall tone of the strategy is defensive in nature and only briefly mentions the capacity for CNA.

The first strategic initiative states the US DOD will treat cyberspace as an operational domain in which to organize, train, and equip its military forces so that it can use cyberspace's full potential.[24] In response, the DOD has established USCYBERCOM, a subunified command under USSTRATCOM, to be responsible for the mission. This includes creating a culture of treating cyberspace as a war-fighting domain as well as establishing active training exercises with red team threats. The second initiative calls for the DOD to employ new defense operating concepts to protect its networks and systems. Achieving this initiative calls for improving configuration management and system updates as well as improving training for DOD members. Additionally, it is developing active defense measures and new architectures.[25]

The third initiative states the DOD will partner with other US government agencies as well as the private sector to provide a whole-of-government approach.[26] This is vital to developing a secure cyberspace that is open and interoperable since different entities own different parts of the US' critical infrastructure. Similarly, as discussed in the NMS, the DOD must build relationships with allies and international partners as the fourth initiative. No single nation or organization owns cyberspace. It is a collective commons used for commerce, communications, and multiple other uses, which are increasing every day. As the last initiative, the DOD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovations.[27] The DOD will invest in its people to facilitate the development of new technology and establish an environment that welcomes innovation.

---

[23] W. Lynn and J. Cartwright, "Defense Strategy for Operating in Cyberspace," (2011).
[24] Lynn and Cartwright, "Defense Strategy for Operating in Cyberspace."
[25] Lynn and Cartwright, "Defense Strategy for Operating in Cyberspace," 6.
[26] Lynn and Cartwright, "Defense Strategy for Operating in Cyberspace," 8.
[27] Lynn and Cartwright, "Defense Strategy for Operating in Cyberspace," 10.

Although these guiding documents on US cyberspace strategy are primarily defensive in nature and focus on resiliency, in 2013 US President Obama made a clear shift towards the offensive use of cyber power. After reviewing international law, President Obama's advisors concluded he has the right "to order a preemptive strike if the United States detects credible evidence of a major digital attack looming from abroad."[28] The government will be developing new policies to include this preemptive option as well as how to govern CNE for signs of potential attacks on the United States. Although the US DOD is capable of conducting CNA operations, this is one of the first clear sign of US policy shifting towards an offensive posture.

United States' Cyber Capabilities

The United States' cyber capabilities are organized under various government entities protecting different aspects of the network based upon who owns that portion of the network. There are multiple organizations responsible for various aspects in cyberspace adding to its complexity. The three primary organizations are the United States DOD, the National Security Agency, and the Department of Homeland Security. As a group, they execute the CNA mission, CND of military and government networks, and the CNE mission. The defense of the remainder of the US cyber infrastructure is the responsibility of the individual owners. These various and distinct entities create a divide in a unified cyber defense for the United States.

The US DOD has organized its military cyber capabilities under United States Cyber Command (USCYBERCOM), which, as previously mentioned, is a subunified command under United States Strategic Command. USCYBERCOM is comprised of units from the Air Force, Army, Navy, and Marines and currently has some 6000 personnel assigned to it. The United States plans to expand the size of this command to 14,000 people over the next few years, which will more than double its current personnel strength.[29] The mission of USCYBERCOM is: "to plan, coordinate, integrate, synchronize, and direct activities to operate and defend the Department of Defense information networks and when directed, conduct full-spectrum military cyberspace

[28] David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," New York Times(2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=1&_r=1&ref=us (accessed 17 February 2013).
[29] Robert K. Ackerman, "U.S. Cyber Force to Grow to 14,000 People," *SIGNAL ONLINE* (2013), http://www.afcea.org/content/?q=node/10622 (accessed 17 February 2013).

operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[30] The units under USCYBERCOM perform both the CNA mission and active CND on military networks. Passive CND units are scattered throughout the DOD and are the responsibility of the individual services, not USCYBERCOM.

Other organizations are further responsible for different missions and the defense of their networks. The NSA performs the CNE mission in support of its overall signals intelligence mission for foreign intelligence and counterintelligence purposes.[31] The DHS is responsible for the protection and defense of the .gov domain and for assisting private sector owners with their expertise.[32] Additionally, majorities of the United States networks are privately owned, and each is responsible for the protection of its own networks. In the United States, this includes the various Internet Service Providers, banks, hospitals, electric, and other critical infrastructure. While US leaders desire an open and free cyberspace where people can express ideas freely, they also desire security, which requires a level of control over cyberspace to help protect the privately owned critical infrastructure that is vital to the state's security.

Coordination between these various organizations is difficult and leaves seams for an adversarial attack. In addition, each organization has a different level of capability to detect and monitor, as well as respond to activities on its network. With the speed of actions in cyberspace, these various seams leave the United States at a disadvantage compared to China with respect to coordination of actions. Since China owns all of its networks and controls everything on them, their required coordination is less. Furthermore, China's use of its cyber militia decentralizes its control more effectively than the United States. As long as the militia is working toward China's overall goal, Chinese leaders do not appear to care how it is accomplished.

[30] "U.S. Cyber Command Fact Sheet," http://www.stratcom.mil/factsheets/cyber_command/ (accessed 17 February 2013).
[31] "NSA Mission," http://www.nsa.gov/about/mission/index.shtml (accessed 17 February 2013).
[32] "Department of Homeland Security: Secure Cyber Networks," http://www.dhs.gov/secure-cyber-networks (accessed 17 February 2013).

Recent US exercises further show US cyber capabilities. In 2012, the US DOD executed its second Cyber Flag training exercise.[33] The exercise included 700 participants from each of the four service components, which more than doubled the number of participants from the previous year. This provided the members the opportunity to practice coordination among the components as well as practice their tactical skills in a role as part either of a US team or as an adversary.

The DHS also participates in annual exercises. In 2006, the DHS led the first annual Exercise Cyber Storm, which was the first government led cyber exercise of its kind. Cyber Storm "simulated a large-scale cyber campaign affecting and disrupting multiple critical infrastructure elements, primarily within the energy, IT, and transportation sectors, and secondarily within telecommunications."[34] Over 115 federal, state, and local governments and private sector companies participated with a focus on interagency coordination. As the first exercise of its kind, there were multiple findings especially related to interagency coordination and the response to multiple cyber incidences, although the response to isolated cyber attacks was proficient.[35] The findings from CYBER STORM III in 2010 were similar, but showed improvement in coordination.[36] However, the final report noted the need for even greater improvement. CYBER STORM 2011 and 2012 were joined exercises building upon one another. While the final report is not complete, the objectives for the exercise included focusing on the findings from CYBER STORM III.[37]

Summary

Understanding the United States strategic and military goals is important for determining how useful a first-strike stratagem would be. The 2010 NSS outlines four primary strategic goals for the United States. The goals include, "The security of the United States, its citizens, and US allies and partners; a strong and growing US economy; respect for universal values at home and around the world; and an international order that

[33] Tech. Sgt. Scott McNabb, "AFCYBER Takes Part in Second USCYBERCOM Cyber Flag Exercise," http://www.24af.af.mil/news/story.asp?id=123327388 (accessed 17 February 2013).
[34] "Cyber Storm Exercise Report," ed. Department of Homeland Security National Cyber Security Division (2006), 4.
[35] "Cyber Storm Exercise Report," 6-9.
[36] "Cyber Storm III Exercise Report," ed. Office of Cyber Security and Communications National Cyber Security Division Department of Homeland Security (2010).
[37] "Cyber Storm: Securing Cyber Space," http://www.dhs.gov/cyber-storm-securing-cyber-space (accessed 17 February 2013).

promotes peace, security, and opportunity through stronger cooperation to meet global challenges."[38] The US NMS goals are to counter violent extremism, deter and defeat aggression, strengthen international and regional security, and shape the future military force. The highlighting feature of these documents is its tone of international cooperation and working with others to achieve these goals. While US leaders state the United States reserves the right to self-defense if attacked, the primary aspects of the document focus on improving defenses, resiliency, and enhancing cooperation to ensure stability. The cyberspace strategies are also of a defensive nature and the US DOD is committed to treating cyber space as an operational domain and developing new defenses to protect it. It is also very collaborative in nature, discussing a whole of government approach to further the workforce as well as technological innovation. A shift in strategy has recently occurred through the 2013 declaration by the Obama administration stating a right to preemptive strikes in cyberspace. This is markedly a different tone than the previously published strategic guidance.

The United States has a robust cyber offensive capability. Although the DOD did not create USCYBERCOM until 2009, the United States has had offensive cyber capabilities long before the creation of this subunified command. The United States is increasing its focus on cyberspace as shown by the addition of 8,000 people to its current manning of roughly 6,000. Furthermore, the addition of the Cyber Flag and Cyber Storm training exercises show the increased emphasis on the operational use of cyberspace by both the DOD and DHS.

[38] Obama, "National Security Strategy," 17.

Chapter 4
First-strike Stratagems

First-strike refers to the advantages accruing to the side in conflict that acts first. The advantages are the ability to use all of one's force (without having to first weather an adversary's attack) and to choose the time and place of the strike. In general, there are two forms of first-strike attacks, either taking an action preemptively or preventively. A preemptive attack is used when an adversary has made clear its decision to attack, has substantially prepared itself to do so, and the attack is *imminent*. Under these conditions, first-strike is generally considered acceptable even under the most restrictive interpretations of just war theory. Preventive action is used when an attack by a potential adversary is not imminent, but there is reason to believe that should the adversary achieve the capacity for first-strike it may well do so. Most theories of just war do not accept preventive action as justifiable. A state's leaders can use a first-strike stratagem for deterrence, coercion, or as a use of force.

The use of a first-strike stratagem to deter an adversary is based upon the idea that the threat of pain and the power to hurt is often times more powerful than hurt itself.[1] In general, deterrence relies on the capability and will of the state making the threat as well as the target state's perception of the threat's credibility. The level of danger felt by the adversary, which comes from the threat of pain coupled with risk tolerance, adds to the deterrent's effectiveness. A leader can increase the likelihood of deterring another state through brinksmanship and increasing the danger of the threat and/or the likelihood of threatened actions occurring.[2] Alternatively, state leaders can use deterrence by denial to reduce the reward of any action or the probability of any action succeeding. The hardening of servers or adding layers of defense are two commonly used tactics to achieve deterrence by denial in cyberspace.[3] The concept of deterrence also relies upon the assumption that states' leaders are rational actors, meaning they make "consistent,

[1] Thomas C. Schelling, *Arms and Influence*. (New Haven, CT: Yale University Press, 2008), 6-8.
[2] Schelling, *Arms and Influence*, 91.
[3] Edward G. Amoroso, *Cyber Attacks : Protecting National Infrastructure*. (Burlington, MA: Butterworth-Heinemann, 2011), 109.

value maximizing choices within constraints."[4] Rationality in this sense does not mean sane or particularly astute, simply that the decision-makers will select among known options the one they believe is most advantageous. While their choices may not appear to make sense to some leaders, their choices are rational when looked at from that leader's perspective. The difference between the views is that calculus for what is best for them and their state depends upon their perceptions, which will most likely vary from those of the leaders of the opposing state.

With respects to conventional deterrence, scholars do not agree on specifically what capabilities are required to create a credible threat.[5] What they do agree upon is in the situation of a significant military imbalance of forces, the leaders of the state with the preponderance of forces will see "that an offensive military strategy can be successful at low cost."[6] This creates a powerful rationale for a first-strike advantage. Nonetheless, it is often found that attackers are overconfident in their ability to translate a military advantage into favorable outcomes, usually because they underestimate the adversary's capacity to resist.[7]

State leaders can also use a first-strike stratagem to compel another state or as force to create an effect. Compellence "induces a state into action or acquiescence by an action that threatens to hurt, often by one that could not forcibly accomplish its aim, but hurts enough to induce compliance."[8] The difficulty with compellence is ensuring the threatened action is threatening something the other cares about. Robert Pape breaks compellence into three forms: punishment, risk, and denial.[9] Punishment raises the costs of not complying with the directed action. Risk works by raising the probability of punishment if action is not taken.[10] Denial works by keeping the target state from

---

[4] Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999), 18.
[5] Paul K. Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2, no. 1 (1999): 29.
[6] Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," 30.
[7] Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," 36.
[8] Schelling, *Arms and Influence*, 79-80.
[9] Schelling breaks coercion down into the components of compellence and deterrence, which is used in this essay. Pape refers to Schelling's definition of compellence as coercion. His wording of coercion has been changed to match Schelling's definition for consistency. Robert Anthony Pape, *Bombing to Win : Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 18.
[10] Pape, *Bombing to Win: Air Power and Coercion in War*, 18.

obtaining its political objectives or territorial goals.[11] When the state realizes it cannot achieve its goal, it gives in to the compelling state. Pape argues that conventional compellence by punishment and risk does not work by examining five historic case studies. Compellence by denial, on the other hand, can and often does work.

To determine how a first-strike stratagem for the United States is useful in cyberspace with respect to China's first-strike stratagem, I analyze two cases in which a first-strike stratagem has been previously used or analyzed and determine the surrounding conditions making it effective. Then, in Chapter 5, I consider what parallels can be drawn between the conditions of a useful first-strike stratagem in these cases and cyberspace.

The first case in which scholars have analyzed a first-strike stratagem is with the use of nuclear weapons. With this case in particular, the United States recent declaration of a first-strike stratagem in cyberspace has been justified by claiming its similarity to the first-strike of nuclear weapons. I examine the useful conditions for a nuclear first-strike stratagem to deter and counter the use of nuclear weapons, to deter and counter the use of conventional weapons, and to compel a state to take a desired action.

The second case I consider is the weaponization of space and under what conditions a first-strike stratagem would be advantageous. I examine the useful conditions for a first-strike stratagem to deter and counter the use of nuclear weapons, to deter and counter the use of conventional weapons, to deter and counter the use of a space weapon, and to compel a state to take a desired action.

Nuclear Weapons

Nuclear weapons are of a different nature than other weapons. George Kennan observed that nuclear weapons are not a weapon of war. War should be to fulfill a political aim, but a war with nuclear weapons that leads to annihilation could not possibly fill any political aim. They are simply a means for destruction.[12] This difference in nature is widely perceived because of the psychic, intellectual, and socially understood tradition of nuclear weapons restraint that, since the last days of World War II, has

[11] Pape, *Bombing to Win: Air Power and Coercion in War*, 15.
[12] Campbell Craig, *Destroying the Village: Eisenhower and Thermonuclear War* (New York: Columbia University Press, 1998), 31.

amounted to their nonuse.[13] To date, no other weapon has the proven, dramatic effects of a nuclear weapon. The sheer destruction, instantaneous effects, and lingering fallout of its usage set this weapon apart. The ability to destroy an entire city with one weapon has a different psychological effect on the enemy as well as the population of the state employing the weapon. Although the firebombing of Japan's wooden cities in World War II burned the cities to the ground, and killed more people, than either of the atomic blasts at Hiroshima or Nagasaki, they are not remembered in the same horrific way as those infamous bombs.[14]

In the intervening years, theorizing to ensure nuclear war could not happen became the apex of intellectual activity for security specialists. The threats of nuclear weapons as a deterrent nuclear brinksmanship and to counter an opponent's use of nuclear weapons are two uses of a nuclear first-strike stratagem.[15] The idea behind this type of deterrence was by maintaining the capability to launch a strike within minutes, and threatening the use of a preemptive nuclear strike if faced with an impending nuclear attack, the opposing side would refrain from even challenging it.[16] It would view either the probability of success as low or the costs of an attack as being too high.[17] As a second means, in order to counter the use of nuclear weapons, a state would strike preventively to disarm the adversarial state of its nuclear weapons before it could use them.

The conditions under which these two concepts of first-strike were useful can be seen during the Cold War. In the beginning of the Cold War, when neither the United States nor the Soviet Union possessed an assured second-strike capability (the capacity to annihilate the other regardless of a first-strike attempt), both states' leaders had an incentive to use nuclear weapons first to eliminate the threat from the other state. As the numeric leader in the nuclear arms race until the mid-1960s, US decision-makers had an

---

[13] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1980), 257-61.
[14] Michael S. Sherry, *The Rise of American Air Power : The Creation of Armageddon* (New Haven: Yale University Press, 1987), 317.
[15] Michael S. Gerson, "No First Use: The Next Step for U.S. Nuclear Policy," *International Security* 35, no. 2 (2010): 25-26.
[16] Gerson, "No First Use: The Next Step for U.S. Nuclear Policy," 26.
[17] Robert Gilpin hypothesizes that states will only try to change the international system if the expected benefits exceed the expected costs. Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981), 50.

incentive to try to eliminate the still growing Soviet nuclear threat. Likewise, Soviet leaders also had an incentive to strike preventively, because they realized they were at a disadvantage numerically and feared a US attack. By striking the United States first, Soviet leaders could ensure the use of their limited number weapons and possibly balance the nuclear numbers or, in a best-case scenario for them, get the United States to surrender. The fact that neither side did so in this situation highlights the conditions that deterred both, despite each having an incentive to strike the other first. The states' were not sure they had the capability to carry out a disarming first-strike successfully. If a first-strike of this type failed, the consequences were terrible—a counterstrike and nuclear war. Both states calculated the cost as too high to offset any benefit of attacking.

By the mid-1960's, the Soviet Union achieved effective nuclear parity with the US, and both sides raced to achieve nuclear overkill; the ability to destroy the other many times over.[18] Mutual Assured Destruction (MAD) was the ironic name for the situation when both sides had attained a second strike capability.[19] Under this condition, neither the United States nor the Soviet Union had a probable chance of eliminating the other side's ability to strike back. In this case, the negative consequences of an all-out nuclear war and annihilation were too high if one side did strike first. In essence, if either side struck first, both would be destroyed. There was nothing to gain except the satisfaction that your enemy would die with you. The United States automation of a nuclear response further increased the probability (assuredness) of a nuclear war if the Soviet Union attacked first. Automation took the decision making away from humans and pushed the level of brinksmanship higher, which improved the deterrent effect.[20]

The use of nuclear weapons as a deterrent to the use of conventional weapons is a second, though of more theoretically ambiguous value, use of a nuclear first-strike strategy. By introducing the threat of nuclear weapons, a rational calculus of the potential cost of taking a proscribed conventional action increases dramatically. President Eisenhower based his strategy of massive retaliation upon this theory of deterrence. He reserved the right of the United States to respond to *any* threat or use of

---

[18] L. Douglas Keeney, *15 Minutes: General Curtis LeMay and the Countdown to Nuclear Annihilation* (New York: St. Martin's Press, 2011), 225, 60, 84; Alain C. Enthoven and K. Wayne Smith, *How Much is Enough?: Shaping the Defense Program, 1961-1969* (Santa Monica, CA: RAND Corporation, 2005).
[19] Keeney, *15 Minutes: General Curtis LeMay and the Countdown to Nuclear Annihilation*, 318.
[20] Schelling, *Arms and Influence*, 91.

force against its interests, no matter how slight, with a nuclear strike. In this manner, Eisenhower threatened a nuclear first-strike response to any type of attack by the Soviet Union (or anyone else) to raise the perceived risk and potential costs of such an action.[21] Unfortunately for his policy, the perceived risk for acting against US interests was not increased; it was decreased because the nuclear threat must appear *credible*. If a nuclear threat does not appear as a logical escalatory step in response to aggression—and a nuclear response to any negative action that was not at minimum highly destructive and extremely costly was simply not conceivable—an adversary state's leaders might rationally ignore it, which seems to have been the case. Little by little, inroads were made, violations were ratcheted up, and in the end even large prohibited actions including the isolation of Berlin and the invasion of Hungary were not inhibited be the nuclear first-strike threat. Alternatively, President Kennedy's strategy of flexible response was implemented to increase the credibility of a nuclear response as a deterrent to the use of conventional weapons.

Like Eisenhower, and every American President since, Kennedy never denounced the first use of nuclear weapons as a response to aggression against the US or its interests, but it is generally understood that the conventional affront would have to be extremely destructive and costly in order to be invoked. This leaves an element of ambiguity in the mind of attackers, which they must account for in their risk/reward determinations. It also leaves a state more maneuvering room if another state does attack it. The benefit of leaving the response ambiguous is that the deterrent effect of the risk of the unknown may be greater than the deterrent effect from knowing the red line for what *will* cause a nuclear response. The downside is the area of ambiguity makes it more difficult for the deterring state to determine when to actually respond and carry out the threatened actions.

The threat of nuclear weapons to counter the use of conventional weapons or to compel a state through punishment, risk, or denial are possible uses of a first-strike stratagem. The limited or tactical threat of nuclear first-strike to compel or force another state to comply with its demands has very few historical examples in support of its

[21] Craig, *Destroying the Village: Eisenhower and Thermonuclear War*, 55.

effectiveness.[22] Additionally, the nature of nuclear weapons makes the prospect of escalation to total war likely, further hindering their value in limiting or defusing conventional aggression scenarios. The Korean and Vietnam Wars are cases in point. United States leaders desired to keep the war limited by placing restrictions on the political aims of the war, which resulted in restrictions placed on US forces in order to avoid a nuclear confrontation with the Soviet Union.[23] The preemptive use of force against a state without nuclear weapons would most likely not appear credible or condoned by the international community, and therefore would not be likely unless a state was faced with an existential threat.

Unlike conventional compellence, however, the probable outcomes of the specific types of nuclear compellence are different. The primary condition for their use is the adversary state could not have nuclear weapons; otherwise, the analysis of a first-strike of nuclear weapons to counter and deter nuclear use would apply. Common sense seems to indicate that the threat of nuclear punishment is the most effective because the damage caused is so great; no target state could resist. A state threatening nuclear punishment must be willing to face the political consequences following from its actual use, however, both domestic and international, making its effectiveness suspect. Compellence by denial is less likely to work because the level of destruction is likely to dominate decision making, and overshadow any political objectives at that point. Alternatively, risk strategies may be useful by raising the potential for harm to compel an adversary without taking action.[24]

---

[22] Gerson, "No First Use: The Next Step for U.S. Nuclear Policy," 10. The Cuban Missile Crisis has been used to make the case for nuclear compellence, though the evidence that the threat of nuclear first-strike by the US caused the Soviets to back down is debatable (see Allison and Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*.)

[23] Conrad C. Crane, *American Airpower Strategy in Korea, 1950-1953* (Lawrence, KS: University Press of Kansas, 2000); Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam* (Lincoln, NE: University of Nebraska Press, 2006).

[24] Pape, *Bombing to Win: Air Power and Coercion in War*, 20.

Space Weapons

Space warfare and space weapons are defined and characterized in a number of ways. One is to call any weapon that can target a space asset or space capability a space weapon. Hence, jamming a frequency used by satellites or targeting a space support facility for destruction is considered a space weapon or space warfare, respectively. This characterization is limited, however, because it does not discriminate weapons that operate in and through space to target on the land or sea, and in the air. The latter emphasizes the *means* of an attack rather than the *ends* for characterizing the type of warfare. David Baldwin provided several good examples illustrating this point. He states, "Bombing a library is not called cultural warfare; bombing homes is not called residential warfare; bombing nuclear reactors (with conventional bombs) is not called nuclear warfare; and bombing factories should not be labeled economic warfare."[25] When bombing is done by aircraft, it is properly understood as airpower. If a battleship performs the bombing, it is properly sea power. And if the bombing comes from a ground battalion's artillery, it is properly land power. Following Baldwin's lead, in order to have a space war or weapon, a state must act *in* space or operate *from* space, respectively. The target is irrelevant to the type of weapon or warfare. This definition helps limit the scope of my analysis and makes it more comparable to those in other domains and especially for cyber weapons, which states use in and through cyberspace.

Like nuclear weapons, state leaders think about space weapons differently than terrestrial-based conventional weapons. While some argue that space is a sanctuary that has not been and should not be weaponized, others assert that states eventually weaponized all the other domains and space is no different.[26] State leaders will eventually weaponize space, they insist, especially because many view it as the ultimate high ground.[27] In this view, the state that is first to weaponize space would gain space superiority and ultimately have dominance there. It would then be able to keep others

---

[25] David A. Baldwin, *Economic Statecraft* (Princeton, NJ: Princeton University Press, 1985), 39-40.
[26] Benjamin S. Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space* (Santa Monica, CA: RAND Corporation, 2003), 116-17. Also Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 131-33.
[27] Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (New York: Frank Cass, 2002), 152.

from weaponizing space.[28] Although ground and air weapons may contest this control, these weapons would not enable another state to gain control. The state must have assets operating in space to have space control, just as an army must have boots on the ground to control territory or a navy must have boats on the water to control the seas.[29] Militaries may use space assets to contest control of the air, land, and sea domains, but they cannot control them from space.

Within this logical framework, there are several situations where there is a first-strike advantage in space. In the following pages, I examine the useful conditions for a first-strike stratagem to deter and counter the use of nuclear weapons, to deter and counter the use of conventional weapons, to deter and counter the use of a space weapon, and to compel a state to take a desired action. I first look at each case by starting with the situation where the deterring or compelling state was the first to weaponize and then the case where two or more states have weaponized space at the same time. The primary limitation of this analysis is that there are currently no known weapons in space, thus the arguments for first-strike are purely theoretical but based upon what is scientifically possible.

One of the most prevalent ways people think about space is by linking its use to nuclear weapons.[30] Since the previous case considered the usefulness of first-strike for these, I will assume that the state with space weapons does not have or will not use its nuclear capabilities. This allows me to decouple the analysis of nuclear and space-based deterrence and narrow the analysis to a single independent variable responsible for the conditions of making a first-strike stratagem beneficial. If the state did have nuclear capabilities, and was willing to use them, the analysis would be similar to the nuclear first-strike in the previous section, with space either adding or adding to a second strike capability.

Space Weapons: Countering and Deterring Nuclear ICBMs

Deterring and countering the use of nuclear intercontinental ballistic missiles (ICMBs) from space is the first way a state may find the conditions advantageous to

---

[28] Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, 157.
[29] Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age* (London, New York: Frank Cass), 2005.
[30] Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*, 25.

adopt a first-strike stratagem. The conditions for deterrence by punishment are similar to the fear of punishment in nuclear deterrence, except in this situation the punishment would come by the destruction of its own nuclear weapons rather than those of the adversarial state. State A would threaten the use of space-based weapons preemptive of a nuclear attack by State B. If State B's leaders believed State A had the capability to destroy their nuclear weapons during or shortly after launch the leaders of State B would most likely be deterred by both fear of punishment and denial. They would fear punishment from their own weapons destructing over their own states *and* they would be denied the capability to attack State A based upon the defense provided by the space-based weapon. The speed of an attack from space—along with it being the ubiquitous nature of a weapon system that can strike anywhere on the globe—quickly adds to its credibility. Allowing the space weapon to destroy any pending nuclear launches it detected automatically would add to first-strike deterrent credibility by increasing the level of brinksmanship.[31]

However, if State B's leaders did not believe State A had the capability or will, then the deterrent effect is lost and a first-strike stratagem is not advantageous. This could be due to never having seen the effects of a space weapon and doubt about its capabilities. This could even make State A's first-strike stratagem harmful, and State B's leaders may be enticed to launch a nuclear weapon into space to disable State A's space capabilities. The costs of this form of nuclear launch is likely less than the costs of a nuclear launch against an adversary's territory because it would not kill any people and the radiation effects would be entirely in space. The principle of *jus in bello* dictates a proportional response.[32] If State B calculates the probability of detonating a nuclear weapon in space as high, the likelihood the opposing state will stop its launch as low, and the potential benefits for eliminating State A's space capabilities as high, it may launch first. State A's dependence upon space will increase the relative benefits of an attack for State B. Although an attack of this type will not only affect State A's assets, but also any other state's assets in the region, and an ionization of the Van Allen radiation belts could occur that would cause more far-reaching and long-lasting effects, there are additional

[31] Schelling, *Arms and Influence*, 91.
[32] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2006), 129.

deterring factors involved. State B must be willing to bear the cost of any retaliation, which could range from diplomatic and economic sanctions to kinetic attacks from the international community.[33] The hardening of state A's assets against nuclear attack is the least expensive and most effective means to improve deterrence and lower State B's first-strike incentive.[34]

Threatening to strike any other target as part of the first-strike stratagem would likely not deter a state's leaders who are willing to use nuclear weapons. This follows from nuclear deterrence theory, in that the power to hurt must be more than the state's leaders are willing to bear. A non-nuclear threat to counter a nuclear threat is not likely to succeed. The state's leaders that desire to use nuclear weapons would be willing to risk the retaliation of a conventional war that included the use of space weapons, with the hopes the conventional war would be limited or stopped from the effects of the nuclear strike. Thus, because the expected benefit of a nuclear strike outweighs the expected pain of any space-based attack, the calculus for deterrence fails.

Another way a state's leaders may find utility in a first-strike stratagem for space weapons is to deter and counter the use of an adversarial state's space weapons. Leaders must consider multiple factors when using this form of deterrence. First, different space assets provide states varying amounts of deterrent capabilities depending on their purpose and the level of war. The more hurt a space weapon can cause, the more it is likely to deter. Additionally, deterrence will vary by target and the opponent's willingness to escalate the war. An attacking state will likely destroy the adversary's GPS capabilities early in a war, for example, to limit its navigation as well as use of precision munitions. A state will most likely wait until a war has escalated before targeting another state's early warning missile system because of its likelihood to escalate the war in the early stages. A state's leaders may launch a nuclear attack if it thinks an adversarial state destroyed its early warning system to facilitate an impending nuclear attack.[35]

---

[33] Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca, NY: Cornell University Press, 1999), 70.
[34] James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*, Second edition. ed. (Stanford, CA: Stanford University Press, 2011), 341.
[35] Forrest E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (Santa Monica, CA: RAND Corporation, 2010), x-xi.

Second, the credibility of a first-strike stratagem is at risk if the threat is not proportional to the costs of a strike against its space assets.[36] As previously discussed, a state's leaders are not likely to view a threat targeting a state's industrial centers and workers over the loss of a satellite as proportional since there was no loss of life. Third, when there is a lack of space situational awareness and an inability to know who attacked, a state has an increased incentive to strike first.[37] This lack of SSA also gives a state a better feasibility of executing a surprise attack on another state, further increasing a first-strike advantage.[38] Presently, it would be difficult to distinguish between an attack by a state and naturally caused damage, which could occur for many reasons such as space debris or equipment failure. Fourth, a first-strike stratagem may be difficult if the targeted space asset is commercial and providing capabilities to allies. For example, a communications satellite used for command and control of military forces may be a target held at risk, but it may also be providing necessary services for allied states. If these states do not agree with the target international partners may be lost.

Fifth, the deterrent benefit of a first-strike stratagem will be weak regardless of which state has more space capabilities, leaving both states' leaders with an incentive to use their weapons first to preempt the use of the opposing state's space weapons. If State B has a weaker military, less space capabilities, and thought war was inevitable with State A, it would have a first-strike incentive to limit future damage by affecting the force ratio between the two sides.[39] The desire for damage limitation coupled with a use-it or lose-it situation tips the scales towards a preemptive strike.[40] State A on the other hand, may think a surprise attack would give an increased advantage and ability to attack at low cost while it still held the advantage.[41]

Sixth, the more heavily State A relies upon the space assets, the higher the incentive for State B to strike first.[42] Alternatively, depending upon how reliant State A is on its space assets will affect whether it has a first-strike incentive. If State A's leaders

---

[36] Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, 30.
[37] Johnson-Freese, *Space as a Strategic Asset*, 110-11.
[38] Van Evera, *Causes of War: Power and the Roots of Conflict*, 69.
[39] Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, 28; Van Evera, *Causes of War: Power and the Roots of Conflict*, 69-70.
[40] Johnson-Freese, *Space as a Strategic Asset*, 133, 35.
[41] Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates."
[42] Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, 30.

realize State B has a first-strike incentive with a high probability of success, it also has an incentive to strike in order to protect its assets first a classic security dilemma.[43] Furthermore, in both situations a lack of good space defenses further disrupts stability providing first-strike incentives.[44]

Space Weapons: Countering and Deterring Terrestrial Conventional Weapons

There are also conditions that would make a first-strike stratagem useful in deterring and countering the use of conventional weapons. The primary advantage a first-strike deterrent space threat has over first-strike threats made from the other domains is that the weapons are located in the ultimate high ground. Military leaders realized the advantages of the high ground long before heavier than air flight. Sun Tzu wrote about armies taking the high ground in his discussions of marches, maneuver, and terrain.[45] In World War I, the US Army used balloons for reconnaissance and targeting purposes. Once heavier than air flight was possible, the military began using what was then considered the ultimate high ground for air superiority, reconnaissance, close air support, interdiction, and strategic bombing. Control of the air over a battlefield allows armies and navies to operate without fear from overhead interference. Further, having air superiority and holding this high ground allows forces in the air to contest ground or sea control. Space is a natural extension of this high ground, without the limitations of gravity, providing military forces speed, range, and stealth. "Satellites traverse in their orbits above every nation in the world, usually unnoticed and eluding traditional terrestrial choke points.[46] Everett Dolman suggests the state that can gain control over this high ground by controlling low earth orbit. The state could deny others from

---

[43] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

[44] Johnson-Freese, *Space as a Strategic Asset*, 133.

[45] Sun Tzu made the following statements regarding the importance of the high ground: "If you wish to give battle, do not confront your enemy close to the water. Take position on high ground facing the sunlight. Do not take position downstream." Also "Therefore, the art of employing troops is that when the enemy occupies high ground, do not confront him; with his back resting on hills, do not oppose him." and "In such ground, he who first takes high sunny positions convenient to his supply routes can fight advantageously." Sun Tzu, *The Illustrated Art of War*, 182, 67, 95.

[46] Mark E. Harter, "Ten Propositions Regarding Space Power: The Dawn of a Space Force," *Air and Space Power Journal*(2006), http://www.airpower maxwell.af.mil/airchronicles/apj/apj06/sum06/harter.html (accessed 5 January 2013).

weaponizing space by using space-based laser or kinetic weapons, which would ensure the preservation of the friendly use of space for commerce and exploration.[47]

Preston lists four advantages of space that further explain the advantage of the ultimate high ground and how a first-strike stratagem will aid in deterring and countering the use of conventional weapons. First, space weapons have better access and reach than other weapons.[48] Since there are no over flight considerations in space, space weapons have better access to engage a target. Furthermore, they can also reach global targets from their vantage point. Second, space weapons are more responsive than terrestrial based weapons. "It could take about 20 minutes after release for a space-based conventional weapon to be deployed in the vicinity of a surface target. In contrast, it takes a few days to some weeks for terrestrial weapons to reach a theater of operations from the United States, with long range ICBMs as the exception."[49] In, both of these cases if deterrence did fail, these weapons are ideal to preemptively strike an adversary quickly, while maintaining an element of surprise. Having forward deployed forces would not be a prerequisite to an attack.

Distance from other weapons is a third advantage space weapons have.[50] This great distance between them and other weapons improves the survivability of space-based weapons. Finally, it is difficult to defeat and defend against many types of space-based weapons.[51] For example, a kinetic-energy weapon targeted against a fixed or slow moving terrestrial target is difficult because of the space weapon's high velocity and short time to traverse the atmosphere. These advantages provide a space weapon superiority over terrestrial-based weapons and add to a first-strike advantage to deter and counter the use of conventional weapons. The more leaders fear these, the more their deterring effect will be.

---

[47] Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, 157.
[48] Preston does not mention cyber weapons in his essay. A space weapon does have better access and reach than a cyber weapon since it is not limited to targets connected to cyberspace. Bob Preston, *Space Weapons: Earth Wars* (Santa Monica, CA: RAND Corporation, 2002), 101.
[49] Cyber weapons would be another exception to a weapon that is technically as or more responsive. Legal issues regarding cyber use, however, make this less likely as well. Preston, *Space Weapons: Earth Wars*, 102.
[50] Preston, *Space Weapons: Earth Wars*, 103.
[51] Preston, *Space Weapons: Earth Wars*, 103.

Space Weapons: Compellence

A state can also use a first-strike stratagem in space to compel another state through punishment, risk, or denial.[52] Although not as punishing as a nuclear compellence stratagem, it would be one in which the other state would actually survive to respond to the compellent action and is therefore more likely to be used than a nuclear compellent action. Since space weapons could cause significant damage, quickly, and anywhere across the globe the surprise itself may be enough to compel an adversary to comply with the stated demands. However, a first-strike stratagem to raise the risk of not complying is more likely to be effective. While Pape argues coercion by risk rarely works for methods other than nuclear risk because it is a watered down form of punishment, risk in coercion is actually very similar to the risk of attacking under a deterrent threat.[53] By manipulating the adversary's cost benefit analysis, a risk-based coercion strategy can work in space. Compellent actions taken against an adversary state's space assets could be temporary, which leaves room for escalation and the risk of more punishment.[54] Temporary losses leave the state something quantifiable to regain with compliance. Once a state's assets are destroyed all a state can then do is comply to avoid further damage. Contrarily, they may decide the damage was not really that punishing, and may realize they can withstand more punishment. Pape argues this was the case in World War II with the firebombing of Japan.[55] Finally, a state could use a first-strike stratagem to compel a state by denying its leaders the accomplishment of their strategic aims.

Summary

The use of a first-strike stratagem for nuclear weapons is useful in several situations. The first is to deter and counter the use of nuclear weapons. As seen in the Cold War, when there is a mismatch in capability, both sides have an incentive to strike and counter the opposing state's use of nuclear weapons. However, if either state was unsure of its ability to carry out the first-strike to disarm the opposing state completely,

---

[52] Pape, *Bombing to Win: Air Power and Coercion in War*, 20.
[53] Pape, *Bombing to Win: Air Power and Coercion in War*, 314.
[54] For example, jamming a satellite is temporary and reversible. Blocking the view of a satellite or its access to power will temporarily withhold the capabilities derived from space without damaging the systems.
[55] Pape, *Bombing to Win: Air Power and Coercion in War*, 92-94.

the stratagem worked on that state as a deterrent because of the devastating effects of a counter attack that would surely follow a failed first-strike. The useful stratagem shifted to one of deterrence when both states attained a second strike capability, known during the Cold War as Mutually Assured Destruction, which also gains its deterrent effect from the power of a nuclear weapon to hurt.

The second possible useful purpose of use of a first-strike stratagem for nuclear weapons is to deter and counter the use of conventional weapons. As long as the threat seemed credible, and not completely disproportional to the conventional use it is trying to deter, a first-strike stratagem would be advantageous. Leaving the conventional red line ambiguous has its benefits as well as negative aspects. The preemptive use of nuclear weapons to counter the use of conventional weapons is unlikely, unless used in the face of an existential threat because of the costs incurred from the international communities' view on their use.

The preemptive use of nuclear weapons to compel a state via punishment, risk, or denial is another means to gain a first-strike advantage. State leaders see nuclear punishment as most effective because the damage is so great, although the state must be willing to pay the political consequences of its use. A first-use risk strategy may be useful, while compellence by denial is unlikely to work because the use of nuclear weapons overshadows any political objectives.

The use of a first-strike stratagem for space weapons is useful in several situations. The first advantage is in deterring and countering the use of nuclear ICBMs. The ubiquitous nature of space weapons and speed of an attack add to the credibility of a first-strike stratagem that would deter a state from attempting to use nuclear weapons. Otherwise, the state's leaders risk a preemptive strike that would destroy the nuclear weapons in their state. However, this stratagem is not effective if the state's leaders do not believe the threatening state has the capability or will to carry out the threatened action. If the state threatening a preemptive strike is dependent upon space, both sides have an increased incentive to strike first. To reduce this incentive, the hardening of space assets is the most effective means. Furthermore, threats against non-nuclear targets in this case are unlikely to work because of the cost/benefit calculus.

The second advantage of a first-strike stratagem is to deter and counter the use of an adversary's space weapons, although multiple factors must be considered in its use. Different space assets affect the deterrent ability based upon importance. The credibility is at risk if the threat is not proportional to the costs. A lack of SSA provides both sides a first-strike advantage regardless of which state has more capability. Commercial space assets add to the difficulty of deterrence or force. Finally, if one state relies on space assets more than the other does, *both* states retain a first-strike incentive. One state has an incentive to hurt the reliant state, while the other has an incentive to defend its capability.

Space weapons also benefit from a first-use stratagem to deter and counter the use of conventional weapons because the hold the ultimate high ground. Additionally, a first-strike advantage can be had using compellence. Because these weapons hold the ultimate high ground and can cause significant damage, they can be used for punishment as well as risk, because there is still an unknown aspect about them. However, a denial strategy is likely to be the most useful.

Chapter 5
First-strike Comparisons

To determine how a first-strike stratagem in cyberspace could be useful in countering China's first-strike stratagem I draw upon the cases of first-strike in Chapter 4. By considering the conditions for making a first-strike stratagem effective in these cases, while also considering the specific attributes of cyberspace, I determine how and under what conditions a first-strike stratagem in cyberspace is useful. I also consider the context of both the United States' and China's strategy and capabilities when drawing these parallels. Then, I consider how this stratagem meets the overall goals and tone of US political and military strategy. Finally, I consider how future improvements to attributing actions in cyberspace could affect the usefulness of the stratagem.

Nuclear Weapons vs Cyber Weapons

Before looking at the conditions for first-strike, it is helpful to understand the differences between a cyber war and a nuclear war. While a nuclear war is an end unto itself and fills no political aim, a cyber war fills an aim independently or as an essential part of or campaign within a broader set of war aims. Winfield's category of attacks to meet use of force thresholds highlights additional differences.[1] Although a cyber attack could cause severe damage and kill people, for example through loss of power for hospitals or by setting the conditions for blowing up gas pipelines, the attack will not have the immediacy of nuclear attack. Even though the duration of action may be quick, it may take a while to feel the effects of a cyber attack or people can abate the duration of its effects due to its manmade nature. Alternatively, along with the massive destruction caused by the weapon's detonation, a state will feel the effects of a nuclear attack for a long time due to the radiological fallout from a nuclear strike. A cyber attack may be anonymous and non-attributable making it hard for a state to respond, while a nuclear missile attack would have clear evidence showing which state launched it. This would allow the state's leaders to know who to hold responsible and retaliate against. Additionally, not all assets can be held at risk with cyber weapons as they can be with

[1] Wingfield, "International Law and Information Operations," 527.

nuclear weapons. Nor can a state continuously hold assets at risk.[2] Cyber operators can often only use a cyber weapon one time, and then the adversary develops a counter for it. Ultimately, until a cyber attack can produce the instantaneous devastation of a nuclear attack and a state can clearly attribute the attack, it will not have the same deterrent effect against its use.

The first situation for nuclear first-strike is to deter and counter the use of nuclear weapons. The first condition where the first-strike of nuclear weapons was useful was when neither state possessed a second strike capability. The purpose of a first-strike under these conditions was for each state to use its weapons before it no longer had the opportunity; eliminate the nuclear threat the other state posed, assuming the location of all nuclear weapons were known and could be hit; and annihilate the other state before it had the opportunity to destroy one's own state.

A parallel comparison for first-strike in cyberspace would be to deter and counter the use of China's cyber weapons. If the conditions in cyberspace were like those of using nuclear weapons, each side would have an incentive to strike and use its weapons while it still had the opportunity to eliminate the other state's cyber weapons. Or, if it were somehow possible, the state could take the opportunity to completely destroy the other state using cyber weapons, thereby eliminating any threat it posed. If a cyber war was in this way like a nuclear war, which it is not, the deterrent effect of possibly starting a cyber war would keep both states from striking first. Each state would be deterred by the fear of failing to completely disarm the other state and the risk of the resulting cyber war.

The conditions for first-strike in cyber war and its deterrence are clearly different than those of a nuclear war. To start, the fear of a cyber war would deter neither the United States nor China from striking the other in cyberspace. The state's leaders do not fear a cyber war as they do a nuclear war because of its inherent differences. Until a cyber weapon can create the instantaneous devastation of a nuclear weapon, this will continue to be the case. However, both states would have an incentive to strike first to preempt and counter an *impending* cyber attack. There is a high benefit to either state to strike while it still has the opportunity to use its weapons. Although it is more difficult in

[2] Libicki, *Cyberdeterrence and Cyberwar*, 39.

cyberspace to contemplate destroying another state's capabilities because of its ubiquitous nature, China's architecture does leave some possibilities. For example, China's firewall is the single point of entry and exit to and from cyberspace. By blocking this exit, the United States could eliminate the threat posed from within China's borders. This would also leave access for US leaders to operate within China, at least until Chinese operators blocked all entry into cyberspace within their borders.

The second condition where the first-strike of nuclear weapons was useful was when one side obtained a second-strike capability. In this case, the state with the second-strike capability had a benefit to strike first without fear of retaliatory strikes. The purpose of a first-strike in this case is to eliminate the nuclear capabilities of the other state. Although, as in the case before, if the state did not believe it could fully disarm the other state, the first-strike utility was eliminated and the state was deterred by the potential costs of a (nuclear) war. The state without a second-strike capability would be deterred regardless and never have a first-strike incentive.

In cyberspace, this scenario is different and both sides would maintain an incentive to strike first to counter the other state's cyber capabilities even if the other state has a second-strike capability. As before, now both sides have an incentive to try to eliminate the other's capability before its own capability is gone. This is because the side without a second-strike capability does not necessarily fear a cyber war, similar to the last deterrent situation.

The deterring capability of a cyber weapon is most likely not great enough because of the difficulty with attribution and the current lack of fear of a cyber war. Thus, even when the problem with attribution is resolved, until the devastating effects of a cyber war are accepted, it will not be feared. Furthermore, a state may not be able to deter another state in cyberspace because it cannot hold its assets at risk repeatedly with cyber weapons. A shift in thinking to fear a cyber war will likely only happen after a crisis. Thomas Kuhn states that only after a crisis will there be a paradigm shift toward new ways of thinking.[3] The world has not yet seen the type of crisis required for this shift to occur.

[3] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: University of Chicago Press, 1996), 66-90.

The fact that the incentive for first-strike remains regardless of a differential in capability is important for the US stratagem. This removes the variable of who has more capability, leaving a first-strike stratagem as useful. Additionally, it is difficult to determine the exact cyber capabilities of a state, because states keep these capabilities hidden. Cyber weapons' one-time use limitation is one of the primary drivers of the need for secrecy. Furthermore, defensive capabilities to achieve deterrence by denial are not currently very robust as demonstrated by multiple incursions into US cyber systems. This can be seen as true concerning China and the United States. While the United States has a higher offensive capability than China (due to its restrictive access, making a concentrated attack possible), its defensive capabilities are much lower.[4] Thus, in cyberspace the United States has a clear incentive to use its capabilities first, before China can attack along its weaker defenses. If the United States does not attack first, China will most likely attack and then cut its network off from the rest of the world via its firewall, making any retaliatory attack by the United States useless. The opportunity will be gone. This is even more critical for the United States because of its heavy dependence upon cyberspace. If it does not adopt a first-strike stratagem, it will suffer comparatively more than China, who is less dependent upon cyberspace.[5] Further, the United States is in a losing situation without cyber, in the face of China's first-strike stratagem.

The third condition gave both sides an incentive for first-strike, but because each had a second strike capability the stratagem was useful for deterrence. The potential probability for a nuclear war was much higher if both sides could strike back, which increases the costs exponentially. Again, the probability of deterring a cyber attack with the threat of a cyber attack is not high, even if both sides have a second-strike capability. This eliminates the first-strike stratagem for the purpose of deterring a cyber attack and war. The cyber threat posed by the United States has not deterred China's leaders, proven by the constant onslaught of cyber attacks from China on the United States.[6] Again, the first-strike stratagem is useful for preemptively countering an imminent cyber attack by attacking the other state first to destroy its capabilities.

---

[4] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*, 148.
[5] Clarke and Knake, *Cyber War: The Next Threat To National Security and What To Do About It.*, 148.
[6] Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 67.

The fourth situation for the first-strike of nuclear weapons was as a deterrent and to counter the use of conventional weapons. As long as the threat seems credible, this threat was useful for deterrence. Although leaving an ambiguous line for countering the use of conventional weapons is not as clear as defining the state's red lines and an adversarial state's leaders could interpret this in an unexpected way. As long as the other state did not have nuclear weapons, the use of them to counter conventional weapons could be useful, but the international community may not see a nuclear response as appropriate.

The first-strike of cyber weapons as a deterrent and to counter the use of conventional weapons is different from how nuclear weapons deter them. First, the threat of using cyber weapons against a non-nuclear state is more credible than threatening to use nuclear weapons against a non-nuclear state for a conventional attack. The punishment is more fitting for the crime. The problem is that most state leaders do not consider a cyber weapon to be as destructive as a conventional weapon, with many considering it an escalation from cyber war.[7] A cyber weapon will therefore not currently deter leaders who are considering a conventional attack. In their minds, they have already escalated *past* a cyber war. This makes a first-strike stratagem in cyberspace as a deterrent to conventional weapons not very useful. On the other hand, state leaders may use cyber weapons to counter the use of conventional weapons preemptively. Unlike nuclear weapons, whose use may be considered negligently violent, even in preemption, a cyber weapon appears to be a more proportional response to an imminent conventional attack. A state's leaders could even use a cyber weapon without anyone knowing who did it because of its anonymous nature. The primary drawback is that cyber weapons cannot counter every conventional weapon directly, as a nuclear weapon can. Conventional weapons that are networked are a primary target for direct attack, while other conventional weapons must be countered through indirect means. Disrupting necessary operational software is one means to counter a conventional weapon, while disrupting command and control could be an indirect means.

[7] Richard Clarke, "War From Cyberspace," *The National Interest* 1(2009): 32. See also Libicki, *Cyberdeterrence and Cyberwar*, 120-21.

The fact that cyber weapons cannot deter the use of conventional weapons can be seen in the relationship between the United States and China. If China invaded Taiwan, and simply threatened the United States with a cyber weapon, the United States would most likely not be deterred from going to Taiwan's defense. China could use its cyber weapons to counter America's use of conventional weapons preemptively, and would probably do so initially in an indirect manner. By attacking the United States' force generation capabilities, the Chinese would at least slow the US militaries' ability to deploy and attack, and probably without international condemnation—at least for the cyber attac. The same situation applies if reversed. The United States could not deter China from attacking strictly by means of a cyber threat. China, however, does have an advantage over the United States concerning a direct cyber attack. Since the PLAs view merges electronic warfare with cyber attacks, its ability to control the EMS is greater than the United States. The US military keeps cyber operations and EW as distinct missions, with little overlap.[8]

Since it has been determined that cyber weapons are not like nuclear weapons, there is little likelihood that similar methods of coercion will work. In fact, the first-strike of cyber weapons for coercion should more closely follow the conventional model where punishment rarely succeeds, risk strategies will fail, and denial strategies work best.[9] This turns out to be true, except for the use of coercion through risk. First, since cyber weapons have thus far not proven themselves as destructive as nuclear weapons, the state will still be able to resist coercion through punishment. This will remain the case until someone proves a cyber weapon can have a long lasting, devastating effect that a state and its population feel immediately. Once this is accomplished, coercion via punishment may work. Another problem with coercion in cyberspace is the lack of an ability to hold a target at risk. After a cyber attack, a state can recover and protect itself from future similar attacks. This makes punishment-based coercion even more difficult.

Second, where cyber weapons could be used is to attempt coercion via risk. While nuclear weapons raise the risk of not complying through their destructive nature,

[8] Joint Publications refer to EW and cyber operations in separate documents. Joint Publication 3-13-1, *Electronic Warfare*, 25 January 2007. And Joint Publication 6-0, *Joint Communications System*, 10 June 2010.
[9] Pape, *Bombing to Win: Air Power and Coercion in War*, 20.

the precise, fast, and unknown nature of cyber weapons increases the risk of non-compliance of a target state. Although no one has proven a cyber weapon to be as destructive as a nuclear weapon, there is still a lot about cyber weapons that are unknown. The coercive act would need to be painful, which gives credibility to a fear of the unknown. Lastly, unlike a nuclear weapon that would have a hard time coercing by denial a because of its sheer destructive nature which divorces it from political aims, a cyber weapon can readily be used. A cyber weapon is a very useful tool that state leaders can use to push another state's leaders further from their aims and towards the realization of the futility of further resistance.

Space Weapons and Cyber Weapons

Space weapons and cyber weapons are more similar than nuclear weapons and cyber weapons. The fundamental similarities between cyberspace and space help drive the conditions for a first-strike advantage. By comparing the weaponization of space and first-strike using space weapons to cyberspace, notions of when a first-strike stratagem would be useful and the conditions surrounding its use can continue to be refined and validated.

Space and cyber weapons are similar because of their ubiquitous nature. The speed with which a state can use them is also similar, although cyber weapons are typically much faster since they can reach around the world at the speed of light. Additionally, both weapons can be stealthy, more so by nature than other kinetic weapons.[10] Furthermore, both weapons have an anonymous nature, which allows their use without attribution in many cases. Finally, unlike nuclear weapons, state leaders use space and cyber weapons to fulfill political aims. They are not an end unto themselves.

The first situation I considered in space was deterring and countering the use of nuclear ICMBs using a first-strike stratagem. This stratagem would be useful for deterrence by punishment and denial as long as the target state believed the defending state had the capability and will to execute a preemptive strike. The speed of a space attack, its ubiquitous nature, and the relative ease of hitting ground targets add to its credibility, while the fact that a space weapon's effects may not yet have been

[10] Exceptions for stealth technology-enabled platforms, such as the B-2 bomber, are not listed as such stealth technology is not domain specific.

demonstrated add doubt to whether the state is capable. The target state may even decide to launch a nuclear weapon into space to destroy the deterring state's space weapon if it perceives that it can do so successfully with low cost. In this case hardening of space assets—making them resistant to nuclear blast effects including irradiation and electro-magnetic pulse—is the best way to improve deterrence through denial. Notably, a first-strike stratagem would probably not be useful in deterring nuclear weapons by threatening to strike any other target other than the nuclear capability itself.

If the conditions for a first-strike advantage in space are like cyberspace, then a cyber weapon should be able to deter and counter the use of a nuclear weapon. Although cyber and space weapons are both fast and ubiquitous, this is simply not enough to make a cyber weapon able to deter a nuclear weapon. There are three primary conditions contributing to this failure. First, like a space weapon, a state has yet to feel the devastating effects of a cyber weapon. Until a state's leaders make the effects of cyber weapons clear, its deterrent effects are highly doubtful. Second, while a space weapon used to deter a nuclear weapon would either be kinetic or have kinetic effects, a cyber weapon has no known direct link through cyberspace to shut down the launch of a nuclear weapon.[11] Unlike Stuxnet, which was executed through an air gap method of attack, a state would not have time to use the same technique during a potential nuclear attack.[12] This greatly undermines the credibility of any deterrent threat, and makes the preemptive countering of a nuclear launch almost impossible. Third, like space weapons, holding another target at risk would not make the cost high enough to a state that is willing to use nuclear weapons. Thus, in the case of nuclear weapons a first-use stratagem would not help and may hinder future deterrent threats made by that state.

The second situation included using a first-strike stratagem for space weapons to deter and counter the use of space weapons. This form of deterrence varied by the targeted system as well as the type of weapon, the proportionality of the threat, the capability of space situational awareness, the use of commercial assets, its space capabilities, and the state's reliance upon space assets. If the same conditions apply to

[11] Even if a cyber method for shutting down a nuclear launch *could* be found, it would not be deterring as it would likely be kept secret until required for use, given the capacity to counter cyber threats after first use. In this case, the cyber attack would be defensive only, with no deterrent capability.

[12] Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 104.

cyberspace, then a first-strike stratagem for cyberspace deterrence should also vary by these factors. First, it should be true that the more hurt a cyber weapon can cause, the more likely it is to deter. Although, as stated before, until a state proves the lethality of a cyber weapon it is not likely to be feared. Second, it should be true that deterrence will vary by the asset the state is trying to protect and the opposing state leader's willingness to escalate a war. This statement is also true for cyberspace. A state may attack military targets first, before it is willing to attack another state's critical infrastructure, for fear of escalating a cyber war into a conventional war.

This can be seen in the hypothetical situation between China and the United States. If China decides to invade Taiwan, it may strike the United States military's command and control structure through cyberspace and attempt to take Taiwan before the United States can respond. In this situation, US leaders would have to evaluate whether the American public had the will to enter into a conflict to free Taiwan. However, if China had successfully attacked the United States civilian power grid, or its banking and trade infrastructure, the American people would likely call for some form of action against China, possibly including a major power war. Thus, the US infrastructure has a higher deterrent capability and is less likely to be attacked if China wants to keep the war as limited as possible.

Third, it should be true that the credibility of a first-strike stratagem for deterrence is at risk if the threat is not proportional to the costs of a strike against the state's cyber assets. This is true and is very much like space. Holding cyber assets at risk has a direct tie to the threat, increasing its credibility. Fourth, the first-strike advantage to counter cyber weapons should increase when there is not a means for attributing attacks. Cyber weapons are very much like space weapons in this regard, although methods of attribution are improving. As long as a state thinks it can strike with anonymity, it will. Additionally, like space, sometimes it is difficult to determine if a problem in cyberspace was due to an attack or a normal software or hardware malfunction. The difficulties with classifying actions in cyberspace as attacks or espionage, for example, further add to a state's first-strike advantage.

This first-strike advantage is the clearest concerning China. Both it and the United States feel they can attack the other and gain an advantage by striking first

because of the attribution problem in cyberspace. If a state cannot prove who or what attacked it, then the state to strike first can likely accomplish its aim before the target state figures out it was an attack rather than a technical problem. Further, China realizes the United States does not have clear boundaries on what constitutes an attack or what an appropriate response is. This increases the likelihood that China could attack with little fear of reprisal should the attack be attributed to it. Although it is not known how China classifies different types of cyber operations, since it is a dictatorship, public support is less necessary, and it is more likely it will respond to an attack. Democracies are much slower to respond to threats and attacks because of the inherent processes built in.[13]

Fifth, if a first-strike stratagem in cyberspace is like one in space it should be true that a first-strike stratagem to counter the use of a cyber weapon will be difficult if commercial assets are involved. This is a very valid prospect in cyberspace because of how people built it, which includes cyber traffic passing through various owners' hardware. Adding to this difficulty is traffic passing through various states on its way to the destination, which adds legal difficulties to using cyberspace to deter or attack a state. A state's leaders will have to weigh the risks of using or damaging a third party in a cyber attack, especially if the state's leaders announce a deterrent threat and must then carry it out.

In the context of the United States versus China, this problem is diminished. Any targets that United States leaders decide to attack in China are ultimately under the control of the state, including its fiber optic infrastructure. However, in the adoption of a first-strike stratagem US leaders must be ready to deal with the issue of traversing third party states. Although the issue is not pressing if China does not attribute the traffic to the United States, it will not be this way for long. If it is important enough to strike a target in China preemptively, US leaders should be willing to travel through other states' cyberspace. Although, as the sole superpower, the international community expects the United States to lead when following and developing international norms of state sovereignty. The United States could lead an effort to develop rules and procedures similar to the rules and procedures to obtain over flight of foreign countries although—

[13] S. Clark and W. Teachout, *Slow Democracy: Rediscovering Community, Bringing Decision Making Back Home* (White River Jct., VT: Chelsea Green Publishing Company, 2012), 114.

and until—the anonymous use of cyberspace is solved it is unlikely to help hinder aggression.

Sixth, if first-strike in cyberspace is similar to space, then the deterrent effect of a first-strike stratagem will be weak regardless of which state has more cyber capabilities, but the first-strike advantage to counter the use of cyber weapons is high for both sides. In this case, the conditions in cyberspace are similar to space. If a less capable state's leaders believe war is inevitable, they would have a first-strike advantage to try to limit future damage from the opposing state. Additionally, they would have a drive to strike before they lost their capabilities because of the inherent vulnerabilities of cyber with the offense currently being stronger than the defense. The more capable state's leaders would want to strike while they have the capability advantage to help limit losses, which gives them an incentive to strike first as well.

The United States and China would both have a first-strike incentive in this situation as well. In particular, the US military is in most ways more advanced and capable than China's military, although vastly it outnumbers the United States in personnel. China's leaders would want to strike the United States and diminish whatever capabilities they could with the hopes of limiting the amount of future damage. This advantage falls directly in line with their INEW strategy to use cyberspace early in a conflict to gain control of the EMS before using kinetic forces. Alternatively, the US has a clear incentive to strike first while its leaders perceive they have an advantage to limit losses. However, the more striking argument for the need for a first-strike stratagem is inherent in its dependence on cyberspace.

Seventh, if first-strike in cyberspace is similar to space, then the more dependent a state is on its cyber capabilities, the more the opposing state has a first-strike advantage to counter the use of cyber weapons. This too, is similar to space. The more dependent another state is on its cyber capabilities the more the opposing state will gain if those capabilities are taken away, giving it a very compelling first-strike advantage.[14] Alternatively, a state highly dependent upon its cyber capabilities also has a larger incentive to strike the other state first to avoid losing those capabilities. As in the previous situation, the weak state of cyber defenses adds to this first-strike advantage.

[14] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 98.

The United States dependence upon cyberspace for its military capabilities such as command and control and its war-fighting generation capability, which relies on the nation's transportation infrastructure, is extensive. A strike on this infrastructure would make it difficult to move people and fuel effectively.[15] Indeed, America's reliance on real-time command and control for critical missions has changed the way leaders make decisions. If their ability to monitor and intervene in events immediately were severely restricted, they may become extremely risk averse in their decision-making. The US militaries' reliance on these cyber dependent capabilities clearly gives its leaders an incentive to strike China preemptively. If the United States military waits and allows China to strike first, it may lose the capabilities it needs to fight. Additionally, it may lose any cyber capabilities to retaliate. With the speed of operations in cyberspace, the cyber war could be over before the target realizes it occurred. Furthermore, since the United States relies on cyberspace more than China, it will lose relatively more than China would from the United States attacking it. This gives China a clear first-strike incentive.

Deterring and countering the use of conventional weapons is the third situation that benefited from a first-strike stratagem in space. As discussed in the section comparing nuclear and space weapons, cyber weapons would not work well as a conventional deterrent until a state proves it can have a highly destructive, kinetic type effect. A state's leaders could use cyber weapons in certain cases to counter the use of conventional weapons. The takeaways from the comparison with nuclear weapons also apply here. In addition, there are many parallels between the advantages of the high ground that drove a first-strike advantageous in space and the advantages that make first-strike advantageous in cyberspace. It provides better access and reach, better responsiveness, and makes it difficult to defeat and defend against cyber weapons.[16] While space provides better access and reach than cyber, simply due to cyberspace being partially manmade and only existing where people want it to exist, it does not reach absolutely everywhere like space does. A weapon in cyberspace does travel faster than a

[15] Herbert Lin, "Operational Considerations in Cyber Attack and Cyber Exploitation," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 38.
[16] These are the reasons for the advantage of the high ground in space. Preston, *Space Weapons: Earth Wars*, 101-03.

space weapon, although the effects of a cyber weapon could be slower. For example, the worm Conficker multiplied very quickly, but it still took days to have a large effect.[17] Additionally, the offensive nature of cyberspace along with its speed and stealth make it very difficult to defend against cyber weapons. All of these advantages help explain China's preference for a first-strike stratagem to counter the use of conventional weapons. Although China will most likely use an indirect cyber attack to stop the US use of conventional weapons, China's leaders have more options for countering conventional weapons directly with their INEW stratagem. While the United States also has EW capabilities, China holds a distinct advantage to be able to use EW and cyberspace in concert to attack and stop a conventional attack. The United States could also use a first-strike stratagem in this manner, although it would require much greater coordination.

The fourth situation for comparison is the using a first-strike with space weapons compared to cyber weapons to compel a state to take a desired action through punishment, risk, or denial. The comparison here adds only a couple points to consider in cyberspace concerning coercion via risk. While Pape argues coercion by risk rarely works, risk in coercion is actually very similar to the risk of attacking under a deterrent threat.[18] By manipulating the cost benefit analysis, this form of coercion can work in space and cyberspace as well. Unlike nuclear risk-based coercion, compelling actions taken against an adversary state's space or cyber assets could be temporary, which leaves room for escalation and the risk of more punishment. Temporary losses leave the state something quantifiable to regain with compliance. Once a state's assets are destroyed, all a it can then do is comply to avoid further damage—or it may decide the damage was not really that punishing and its leaders may realize they can withstand more punishment. Again, Pape argues this was the case in World War II through the strategic firebombing of Japan.[19] Ultimately, the best method of coercion is still using a first-strike stratagem to compel a state by denying its leaders the accomplishment of their strategic aims.

First-strike and US Political and Military Strategy

A first-strike stratagem should meet US political aims and coincide with US strategy. I assess this by analyzing the key aspects of the US NSS, NMS, and cyberspace

[17] Bowden, *Worm: The First Digital World War*.
[18] Pape, *Bombing to Win: Air Power and Coercion in War*, 20.
[19] Pape, *Bombing to Win: Air Power and Coercion in War*, 92-94.

strategies. This analysis, along with the previous comparisons, allows me to consider the recent statements in the news about the United States' declared first-strike stratagem for cyberspace and its usefulness.

American leaders' are focused on the security and prosperity of the country and its people and fostering a cooperative international community to handle problems together. Within the context of its security, American leaders specifically pointed out their right to use military force in its defense. Although US leaders are welcoming China to participate in the international community and act responsibly, US leaders will be watching its military developments to ensure it is not threatening to the United States and US interests. In this regards, a declared first-strike stratagem to deter China through cyberspace may seem appropriate, however, I have shown deterrence in cyberspace is very difficult to achieve in all cases of deterrence. Further, China does not appear deterred with or without a declaration of first-strike. When this method of deterrence fails, any negative perceptions of a preemptive strike within the international community may ease. On the other hand, the use of a first-strike stratagem as a use of force to counter various weapons is quite useful. When accepting a first-strike policy, the United States should not declare it as such, but keep it secret. A declaratory policy simply alerts the adversary to your intentions, which is not useful in this case, when much of the first-strike advantage comes from surprise.[20]

Although a first-strike stratagem appears to be at odds with the NSS goal of fostering a cooperative international community to handle problems together, there are ways to counter this. A first-strike stratagem may appear as if the United States is flexing its hegemonic status, unilaterally going on its own following the classic realist sentiment from Thucydides, "the strong do what they can and the weak suffer what they must."[21] But this is a situational requirement. As I have shown, a first-strike stratagem is necessary for many situations in cyberspace, especially as a use of force to counter various weapons, and so US leaders have several options that would foster a cooperative community. They could work with select allies and partners to agree to a first-strike stratagem, sharing the analysis and benefits of doing so, and not declaring the policy or

[20] Van Evera, *Causes of War: Power and the Roots of Conflict*.
[21] Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War* (New York: Free Press, 1996), 352.

the partners publicly to avoid limiting its efficacy. The downside to this is that US leaders would not be working with the entire international community; however, having the entire international community's support is unlikely to happen regardless of the situation. The other option US leaders have is to keep the first-strike stratagem secret and work with the international community in other ways to help secure cyberspace for peaceful use. US leaders could also continue working with China in this regard and work towards lessening the threat it poses in cyberspace. The negative aspect to this option is even with the anonymous nature of cyberspace, only certain countries have the capability to carry out certain types of attacks and the US could be seen as acting unilaterally and contradictive to any declarations of a peaceful and secure cyberspace. However, if the US has a strong case for preemptive use it should not be an overly restrictive problem and its allies and partners will view a preemptive attack as necessary for state security. A third option is to avoid a first-strike stratagem all together, which would preclude any appearance of a bully hegemon, which inhibits US leadership in the international community. While this option may work in the short term, it undermines the state's security. Considering the United States' dependence upon cyberspace, ensuring its use is relatively uninhibited is important for its economic, informational, and physical security. China's views on the use of cyberspace in a conflict as well as its views of the US interfering with unification with Taiwan adds to the threat to the state's security.

While the NSS supports the goals above, it also has an additional goal that is worth examining. Military leaders plan to shape the future force, which will enable them to accomplish their missions. In particular, they plan to protect military networks through a resilient architecture that can recover from attacks using detection, deterrence, denial, resilience, and defense in depth.[22] This defensive stance is a good example of the passive, defensive nature of the NSS and NMS. While the US clearly states it will protect itself if attacked, there is nothing to hint at any thoughts of preemption. This stance fits well with the US desire to build norms and standards of behavior in cyberspace, which will help sustain partnerships and rule of law in cyberspace.[23] The

[22] "National Military Strategy," 19.
[23] Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 8.

only options that appear to fit in with these desires is to either secretly adopt a first-strike stratagem and use it only when necessary or to avoid it all together.

Further, the US desire to have an open and interoperable cyberspace raises questions about the usefulness of a first-strike stratagem.[24] The concept of an open cyberspace is not what a state would want if another state had a first-strike stratagem. While it is clear that a declared policy would hamper the ability of states to work toward this goal, the fears of international leaders about the possibility of hidden preemptive stratagems is also detrimental to achieving this goal. The US would have to be open and honest about its capabilities and architecture to instill this type of trust, as would other countries. China's leaders would never be this open with their policies because of its closed society and their current stance toward censoring the information coming into and out of their country. This lack of reciprocal openness will make it hard to achieve this goal. Thus, while an open first-strike deterrent stratagem is clearly a hindrance towards achieving this goal, a hidden first-strike stratagem for force or coercion may be useful if required.

After the publication of the NSS and NMS, President Obama made a clear shift towards the preemptive use of cyber power. The President's advisors concluded he has the right "to order a preemptive strike if the United States detects credible evidence of a major digital attack looming from abroad."[25] While this declares a preemptive strike stratagem, it is not a useful form of the stratagem. A declared stratagem is meant as a deterrent threat. Based upon the case studies herein, cyber is not currently a viable deterrent threat for nuclear weapons, conventional weapons, or even cyber weapons. For the use of a first-use stratagem to counter conventional and cyber weapons a declaratory first-strike stratagem simply puts the adversary on notice so it can prepare. In China's case, its leaders will likely see this as a direct threat because of the Taiwan issue and the US President's declared, "*Pivot to the Pacific",* which constitutes a new focus on Asia.[26] These two signals in concert would

[24] Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 8.
[25] Sanger and Shanker, "Broad Powers Seen for Obama in Cyberstrikes".
[26] Mark E. Manyin, "Pivot to the Pacific?: The Obama Administration's 'Rebalancing' Toward Asia," (Congressional Research Service, Library of Congress, 2012).

make any state stop and take notice, but is the declared first-strike stratagem in this case likely to deter China? I do not think so.

The Future of a First-Strike Stratagem

The landscape of cyberspace is constantly changing and will affect the future usefulness of a first-strike stratagem. There are three changes likely to happen in the near future. First, a cyber weapon will most likely be shown as effective as a kinetic weapon. With more and more aspects of human life linked to cyberspace, the options for targets is likely to grow. Like all other weapons, it is only a matter of time before a state proves its destructive ability. It remains to be seen whether it can cause a long-term disruption of power in the middle of winter, resulting in hundreds of deaths; or if attacks causing financial markets to close or balances in accounts to change will cause chaos and panic in a country. Once a state proves the destructive nature of cyber weapons, they will gain an ability to deter. They will not likely have the ability to deter nuclear weapons, but with an effect on par with conventional weapons, they can deter those and cyber weapons.

Second, attribution in cyberspace is already improving. Although attribution is still difficult, by using a few methods of attribution together, the likelihood of finding an attacker increases. This improvement will raise the risk of using a first-strike stratagem in cyberspace as a use of force. Thus, a state must see a corresponding increase in the benefit of a first-strike before attacking.

Third, cyber defenses may improve. As defenses improve, a first-strike stratagem for deterrence will also improve as the prospects of a successful first-strike decrease. While this improves deterrence, it has the opposite effects on the use of force and coercion. Like attribution, the benefit gained from an attack must increase to outweigh the increased cost of attack.

Summary

The advantage of a first-strike using cyber weapons compared to nuclear weapons is different because of the inherent differences between the weapons. The non-political nature of a nuclear weapon is one of the most glaring differences. However, the instantaneous and prolonged devastation caused by nuclear weapons is also distinctly different. A cyber attack may be anonymous and non-attributable making it hard for a state to respond, while a nuclear missile attack would have clear evidence showing which

state launched it. Not all assets can be held at risk with cyber weapons as they can be with nuclear weapons. Nor can a state continuously hold assets at risk.[27] Ultimately, until a cyber attack can produce the instantaneous devastation of a nuclear attack and a state can clearly attribute the attack, it will not have the same deterrent effect against its use.

The conditions for surrounding a cyber war are different from a nuclear war, making deterrence using a first-strike stratagem not useful, although the stratagem is advantageous in countering a potential cyber attack. Neither the United States nor China are or would be deterred from striking the other in cyberspace because the effects of a cyber war do not have prolonged devastating effects. However, the use it or lose it nature of cyber weapons gives both the United States and China a first-strike incentive. Unlike nuclear deterrence attained with a second strike capability, the first-strike incentive is retained regardless of the states' capabilities because the states do not currently fear a cyber war. The problem with attributing a cyber attack to the attacker adds to the first-strike incentive.

In the comparison of cyber weapons to nuclear weapons, they would not be useful as a deterrent to the use of conventional weapons, but a first-strike stratagem could counter the use of some conventional weapons. Although a deterrent threat of a cyber weapon is more credible in this case and seen as a proportional response, it will not deter a state's leader that is ready to escalate beyond a cyber war, such as a decision by China to invade and reunite with Taiwan. As long as the use of the weapon is either directly or indirectly tied to cyberspace this is a possibility.

The same methods of coercion in cyberspace do not work under a first-strike stratagem as they do for nuclear weapons. First, since cyber weapons have thus far not proven themselves as destructive as nuclear weapons nor able to hold a target at risk repeatedly, the state will still be able to resist coercion through punishment. Second, cyber weapons could be used to attempt coercion via risk through its precise, fast, and unattributable nature. Third, unlike a nuclear weapon that cannot coerce via denial, a cyber weapon would work best under this method of coercion. Pushing China's leaders

[27] Libicki, *Cyberdeterrence and Cyberwar*, 39.

away from their aims and towards the realization of the futility of further resistance is the best and most efficient coercive method.

The advantage of a first-strike using cyber weapons compared to space weapons is more similar than the comparison to nuclear weapons because of the fundamental similarities between the two. Both space and cyber weapons are ubiquitous in nature, fast, stealthy, and can attack anonymously. There are some differences, though, that also drive differences in advantage.

A cyber weapon is not useful in deterring the use of a nuclear weapon for the same reasons it has difficulty deterring a conventional weapon in the nuclear comparison. A first-use stratagem in cyberspace is useful to counter cyber weapons, but is still ineffective in deterring them. The similarities and dissimilarities to space weapons further show where this is advantageous. Like space weapons, deterrence in general does not work well in cyberspace because of attribution, but deterrence will vary by the asset the state is trying to protect and the opposing state leader's willingness to escalate a war. Second, like space, the credibility of a deterrent first-strike stratagem is due to its proportionality. Third, commercial capabilities add difficulties to deterrence and the ability to counter use through force. Fourth, like space, the deterrent effect is weak regardless of capability due to the use it or lose it drive. Fifth, dependence upon cyber capabilities provides both states a first-strike advantage. An important aspect the comparison adds is the ability to take a temporary action in space and cyberspace. This leaves more room for escalation and adds to the uncertainty of risk-based compellence.

A first-strike stratagem should meet US political aims and coincide with US strategy. This is evident through an analysis of key aspects of the US NSS, NMS, and cyberspace strategies. This analysis along with the previous comparisons allows me to consider the recent statements in the news about the United States declared first-strike stratagem for cyberspace and its usefulness.

A first-strike stratagem fits very well with US strategic and military aims, although the various aims each benefit more or less from either deterrent or force stratagems. Although a declaratory stratagem aimed at deterrence is not useful in cyberspace, one that is not declared could be very useful. It could help sustain the security and prosperity of the US as well as foster a cooperative international community

to handle problems. The manner in which the US keeps its policy a secret, even from allies, could affect this cooperation. Additionally, US strategic documents are inherently defensive in nature, and even the aggressive statement of reserving the right to attack at a time and place of its choosing if attacked is defensive. This defensive stance means the US could either try deterrence, hide a preemptive stratagem, or not use a first-strike stratagem at all. Furthermore, the desire for an open and secure cyberspace has implications on the best use of first-strike stratagem with China. Finally, after considering the comparative case studies, the alternate ways to use this stratagem in accordance with strategic aims, and in accord with the United States' pivot to Asia, I have found the US shift toward an announced deterrent preemptive stratagem to be ineffective.

The landscape of cyberspace is constantly changing and will affect the future usefulness of a first-strike stratagem for deterrence. In the future, a cyber weapon will be proven as effective as a kinetic weapon, attribution will improve, and cyber defenses may improve. Each of these developments will add to deterrence by increasing the fear of an attack, being discovered and held accountable, or by denial. Once this occurs, the United States will need to have a declaratory versus a hidden first-strike stratagem.

Chapter 6
Recommendations

Based upon the previous analysis, I recommend the United States adopt a first-use stratagem aimed at countering the use of China's cyber weapons or conventional weapons with an option to use cyber weapons in a first-strike for coercion by denial. This stratagem requires US leaders to keep the stratagem non-declaratory. A declaratory stratagem would make it a deterrent, which is simply not a feasible stratagem at this point in time. The adoption of a first-use stratagem for countering the use of China's cyber weapons or conventional weapons fits the nature of the weapon as well as current US political and military aims.

First, the attributes of cyber weapons lend themselves best to a stratagem of countering the use of force than deterrence. The ubiquitous, speed, deceptiveness, non-attributable, and offensive nature give cyber weapons a clear advantage when used first. Due to the anonymous nature of cyber weapons, deterrence is difficult if clear evidence does not exist showing who attacked. Although cyber weapons can only affect certain conventional weapons directly, there may be ways to affect them indirectly, such as by affecting a state's command and control infrastructure. Since both China and the United States have a first-strike incentive, the best stratagem is to counter the use of cyber weapons preemptively. In the case of China in particular, since it is likely they may strike and then remove their country from the global internet, it is imperative that the United States strikes first with its cyber weapons. Otherwise, it may forgo the opportunity completely.

This stratagem also fits well with current US political and military aims. It could help sustain the security and prosperity of the US as well as foster a cooperative international community to handle problems. I would recommend the US share this stratagem and reasoning behind it with its closest allies. Then, if the stratagem was executed it would not undercut relations with US allies. Furthermore, this stratagem does not take away from US leaders desire for an open and secure cyberspace. The openness of cyberspace has to do with interoperability and the freedom of information to flow

through cyberspace. Thus, having a preemptive stratagem does not counter interoperability, it on seeks to preserve the security of cyberspace. US leaders must realize if they decide to use a cyber weapon in a first-strike they will have to explain and justify its use. Although the anonymous nature of cyberspace may allow the US to hide its actions, there will come a time when it cannot. Thus, US leaders must be willing to accept risks of a first-strike—and use it—knowing it is justified.

In the future, the United States should shift to a declaratory deterrent first-strike stratagem. This can occur once several things have occurred to improve its value as a deterrent. Once a cyber weapon has been proven as effective as a kinetic weapon the fear of its use will increase. When the attribution of cyber weapons improves the probability of being held responsible for an attack increases, raising the cost of an attack. Finally, when cyber defenses have improved, the ability likelihood of an attack succeeding will decrease, affecting the cost/benefit analysis of the attacker. Thus, the cost/benefit analysis of an attacker will shift as attribution increases the cost, while improved defenses decreases the benefit, ultimately improving deterrence.

Bibliography

Ackerman, Robert K. "U.S. Cyber Force to Grow to 14,000 People." *SIGNAL ONLINE* (2013). http://www.afcea.org/content/?q=node/10622.

Air Force Doctrine Document 3-12. *Cyberspace Operations*, 30 November 2011.

Allison, Graham T., and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: Longman, 1999.

Homeland Security Subcommittee: Oversight and Management Efficiency. *America Is under Cyber Attack: Why Urgent Action Is Needed*, 24 April 2012.

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Burlington, MA: Butterworth-Heinemann, 2011.

Andres, Richard B. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.

"Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." edited by Office of the Secretary of Defense, 2012.

"Annual Report to Congress: Military Power of the People's Republic of China 2009." edited by Office of the Secretary of Defense, 2009.

Baldor, Lolita C. "Chinese Cyber Attacks on U.S. Continue Totally Unabated, Leon Panetta." *Huffington Post* (2012). http://www.huffingtonpost.com/2012/09/20/chinese-cyber-attacks-leon-panetta_n_1899168.html.

Baldwin, David A. *Economic Statecraft*. Princeton, NJ: Princeton University Press, 1985.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.

Brenner, Susan W. *Cyberthreats : The Emerging Fault Lines of the Nation State*. New York: Oxford University Press, 2009.

Cartwright, General James E. "Comments." Paper presented at the Air Force Association Air Warfare Symposium, 8 February 2007.

"China's Aging Population to Double by 2053." *China Daily* (2012). http://usa.chinadaily.com.cn/china/2012-10/23/content_15837814.htm.

"China's National Defense 2006." Information Office of the State Counsel, http://www.china.org.cn/english/features/book/194421.htm.

"China's National Defense 2010." Information Office of the State Counsel of the People's Republic of China, http://www.china.org.cn/government/whitepaper/node_7114675.htm.

"China Pla 'Mission Operations 2010a' Military Exercise Started." http://www.chinamilitary.net/china-pla-mission-operations-2010a-military-exercise-started.html.

"Chinese Intelligence Agencies." Global Security, http://www.globalsecurity.org/intell/world/china/index.html.

Clark, S., and W. Teachout. *Slow Democracy: Rediscovering Community, Bringing Decision Making Back Home*. White River Jct., VT: Chelsea Green Publishing Company, 2012.
Clarke, Richard. "War from Cyberspace." *The National Interest* 1 (2009): 31-36.
Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco, 2010.
Clausewitz, Carl von. *On War*. Princeton, N.J.: Princeton University Press, 1984.
Clodfelter, Mark. *The Limits of Air Power: The American Bombing of North Vietnam*. Lincoln, NE: University of Nebraska Press, 2006.
Cooper, Jeffrey R. "A New Framework for Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.
Corbett, Julian Stafford. *Some Principles of Maritime Strategy*. Annapolis, MD: Naval Institute Press, 1988.
Craig, Campbell. *Destroying the Village: Eisenhower and Thermonuclear War*. New York: Columbia University Press, 1998.
Crane, Conrad C. *American Airpower Strategy in Korea, 1950-1953*. Lawrence, KS: University Press of Kansas, 2000.
"Cyber Storm Exercise Report." edited by Department of Homeland Security National Cyber Security Division, 2006.
"Cyber Storm Iii Exercise Report." edited by Office of Cyber Security and Communications National Cyber Security Division Department of Homeland Security, 2010.
"Cyber Storm: Securing Cyber Space." http://www.dhs.gov/cyber-storm-securing-cyber-space.
"Cyberattacks on Critical Infrastructure Increase 17-Fold, Says Nsa Chief." *Infosecurity-magazine* (2012). http://www.infosecurity-magazine.com/view/27275/cyberattacks-on-critical-infrastructure-increase-17fold-says-nsa-chief/.
Denning, Dorothy Elizabeth Robling. *Information Warfare and Security*. New York: ACM Press, 1999.
"Department of Homeland Security: Secure Cyber Networks." http://www.dhs.gov/secure-cyber-networks.
Dicken, Peter. *Global Shift: Mapping the Changing Contours of the World Economy*. 6th ed. New York: Guilford Press, 2011.
"Dictionary.Com." http://dictionary.reference.com/browse/cyber.
Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*. New York: Frank Cass, 2002.
———. *Pure Strategy: Power and Principle in the Space and Information Age*. New York: Frank Cass, 2005.
Enthoven, Alain C., and K. Wayne Smith. *How Much Is Enough?: Shaping the Defense Program, 1961-1969*. Santa Monica, CA: RAND Corporation, 2005.
"European Commission Trade: China." European Commission, http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/china/.

Fidler, David P. "The Law of Armed Conflict and Cyber Conflict." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.
Flew, Terry. *New Media: An Introduction*. New York: Oxford University Press, 2002.
Gerson, Michael S. "No First Use: The Next Step for U.S. Nuclear Policy." *International Security* 35, no. 2 (2010/10/01 2010): 7-47.
Gibson, William. *Neuromancer*. New York: Ace, 1984.
Gilpin, Robert. *War and Change in World Politics*. Cambridge: Cambridge University Press, 1981.
Gjelten, Tom. "Cyber Insecurity: U.S. Struggles to Confront Threat." *NPR* (2010). Published electronically 6 April. http://www.npr.org/templates/story/story.php?storyId=125578576.
Gove, Philip Babcock. *Merriam Webster's Third New International Dictionary*. Springfield, MA: Merriam-Webster, 2002.
Greenert, Jonathan W. "Imminent Domain." *Proceedings Magazine* 138/12/I,318, (2012). http://www.usni.org/magazines/proceedings/2012-12/imminent-domain.
Harter, Mark E. "Ten Propositions Regarding Space Power: The Dawn of a Space Force." *Air and Space Power Journal* (2006). http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/sum06/harter.html.
"Highlights: Chinese Pla's Recent Military Training Activities ". *FBIS Report* (6 June 2004): OSC ID CPP20040619000083.
Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science* 2, no. 1 (1999): 25-48.
"'Iron Fist-2009' Military Exercise in Jinan Mac ". *PLA Daily* (2009). Published electronically 27 November 2009. http://china-defense.blogspot.com/2009/11/iron-fist-2009-military-exercise-in.html.
Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.
Johnson-Freese, Joan. *Space as a Strategic Asset*. New York: Columbia University Press, 2007.
Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 16 November 2009.
Joint Publication 3-13. *Information Operations*, 13 February 2006.
Joint Publication 3-13-1. *Electronic Warfare*, 25 January 2007.
Joint Publication 6-0. *Joint Communications System*, 10 June 2010.
Keeney, L. Douglas. *15 Minutes: General Curtis Lemay and the Countdown to Nuclear Annihilation*. New York: St. Martin's Press, 2011.
Krekel, B., P. Adams, and G. Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." US-China Economic and Security Review Commission. Northrup-Grumman, 2012.
Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." DTIC Document, 2009.
Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.
Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press, 1996.
Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." *Joint Force Quarterly* 60 (2011): 46-53.
———. *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*. Santa Monica, CA: RAND Corporation, 2003.
Lewis, James Andrew. "The Cyber War Has Not Begun." *Center for Strategic and International Studies* (2010). http://dev.csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf.
Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
———. "Military Cyberpower." In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.
Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploitation." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.
Lynn, W., and J. Cartwright. "Defense Strategy for Operating in Cyberspace." (2011).
"Majestic and Powerful Forces, Fierce and Sweeping Actions over a Thousand Miles -- Review of, and Thoughts About, the 'Mission Action-2010c' Trans-Region Mobile Exercise." *Chengdu Zhanqi Bao* (2010): OSC ID CPP20101222478002. https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_0_0_43/content/Display/22118627?returnFrame=true.
Manyin, Mark E. "Pivot to the Pacific?: The Obama Administration's 'Rebalancing' toward Asia." Congressional Research Service, Library of Congress, 2012.
McCarthy, John A., Chris Burrow, Maeve Dion, and Olivia Pacheco. "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts." In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.
McNabb, Tech. Sgt. Scott. "Afcyber Takes Part in Second Uscybercom Cyber Flag Exercise." http://www.24af.af.mil/news/story.asp?id=123327388.
"Merriam-Webster Dictionary." http://www.merriam-webster.com/dictionary/cyber.
"Migration and Movement of People." http://www.chinaonlinecentre.org/china_people_migration.html.
Mitchell, William. *Winged Defense*. Tuscaloosa, AL: University of Alabama Press, 2009.
Moltz, James Clay. *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*. Second edition. ed. Stanford, CA: Stanford University Press, 2011.
Morgan, Forrest E. *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*. Santa Monica, CA: RAND Corporation, 2010.

Mulvenon, J.C., and A.N.D. Yang. *The People's Liberation Army as Organization*. Santa Monica, CA: RAND Corporation, 2002.
"National Military Strategy." edited by Department of Defense, 2011.
"Nsa Mission." http://www.nsa.gov/about/mission/index.shtml.
Obama, Barack. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." 2011.
———. "National Security Strategy." Washington DC, 2010.
Osinga, Frans. *Science, Strategy and War: The Strategic Theory of John Boyd*. New York: Routledge, 2007.
Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.
Perlez, Jane. "China Sends Troops to Disputed Islands." *New York Times* (2012). Published electronically 23 July 2012. http://www.nytimes.com/2012/07/24/world/asia/china-sends-troops-to-disputed-islands.html?_r=0.
Preston, Bob. *Space Weapons: Earth Wars*. Santa Monica, CA: RAND Corporation, 2002.
Proctor, J. *American Resolve and the Art of War: A Study and Application of Military Tactics*. Bloomington, IN: Author House, 2012.
Qingmin, Dai. "Innovating and Developing Views on Information Operations." *China Military Science* (August 2000).
———. "On Integrating Network Warfare and Electronic Warfare." *PLA Academy of Miliary Science and the China Military Science Association* (February 2002).
Raman, Manikandan. "China Makes World's Fastest Supercomputer." *International Business Times* 28, (2010). Published electronically 28 October. http://www.ibtimes.com/china-makes-worlds-fastest-supercomputer-246732#.
Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.
Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.
Sanger, David E., and Thom Shanker. "Broad Powers Seen for Obama in Cyberstrikes." *New York Times* (2013). Published electronically 3 February 2013. http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=1&_r=1&ref=us.
Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.
———. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1980.
Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1995.
Sharma, D. "Integrated Network Electronic Warfare: China's New Concept of Information Warfare." *Journal of Defence Studies* 4 (2010): 38-39.
Sharp, Walter Gary. *Cyberspace and the Use of Force*. Falls Church, VA: Aegis Research Corp., 1999.
Sheldon, J.B. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* (2011).

———. “State of the Art: Attackers and Targets in Cyberspace.” *Strategic Studies Quarterly* (2012).
Sherry, Michael S. *The Rise of American Air Power : The Creation of Armageddon*. New Haven: Yale University Press, 1987.
Simpson, John A, E.S. Weiner, and Michael Proffitt. *Oxford English Dictionary*. Oxford, England: Clarendon Press, 1997.
Smith, I.C., and N. West. *Historical Dictionary of Chinese Intelligence*. Lanham, MD: Scarecrow Press Incorporated, 2012.
Thomas, Timothy Lloyd. *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.
Thucydides. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. New York: Free Press, 1996.
House Committee on Foreign Affairs. *China's Quest for a Superpower Military*, 2007.
Tzu, Sun. *The Illustrated Art of War*. New York: Oxford University Press, 2005.
“U.S. Air Force Shifts 30,000 Troops to 'Cyberwar Front Lines'.” *Homeland Security News Wire* (2010). http://www.homelandsecuritynewswire.com/us-air-force-shifts-30000-troops-cyberwar-front-lines.
“U.S. Cyber Command Fact Sheet.” http://www.stratcom.mil/factsheets/cyber_command/.
Van Evera, Stephen. *Causes of War: Power and the Roots of Conflict*. Ithaca, NY: Cornell University Press, 1999.
Waltz, Edward. *Information Warfare: Principles and Operations*. Boston, MA: Artech House, 1998.
Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books, 2006.
Wheeler, D.A., and G.N. Larsen. “Techniques for Cyber Attack Attribution.” DTIC Document, 2003.
Willson, David L. “Cyberwar or Cyber Cold War?” *Information Systems Security Association Journal* (2012). http://www.titaninfosecuritygroup.com/UserFiles/HTMLEditor/Cyberwar%20or%20Cyber%20Cold%20War_ISSA0912.pdf.
Wingfield, Thomas C. “International Law and Information Operations.” In *Cyberpower and National Security*, edited by F.D. Kramer, S.H. Starr and L. Wentz. Washington, DC: Potomac Books Incorporated, 2009.
Yasar, Nurgul, Fatih M. Yasar, and Yucel Topcu. “Operational Advantages of Using Cyber Electronic Warfare (Cew) in the Battlefield.” Paper presented at the Proc. of SPIE Vol, 2012.
“Country Report: China.” *The Economist*, no. 2 (2012): 1-28.